Q-NET POINT-TO-MULTIPOINT

WIRELESS ACCESS SYSTEM

Product guide

document version PRX0045-10

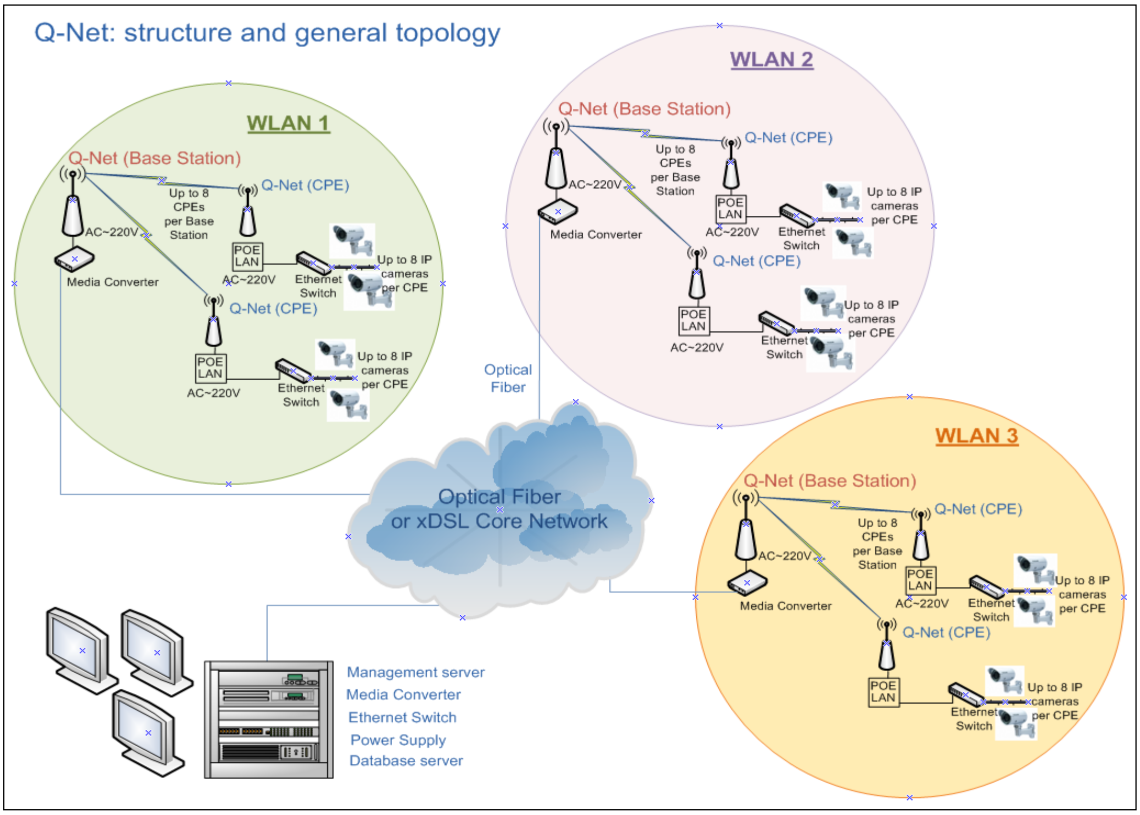
Overview

Q-Net is an integrated system aimed to provide for reliable wireless data transmission links for digital video surveillance cameras spread across any specific area like city, village, industrial plant, etc, and where traditional SHDSL or fiber optic links are unavailable or difficult to provide due to technical limitations. From the network topology point of view, Q-Net is a combination of multiple subsystems using uniform access layer and controlled from the central monitoring center.

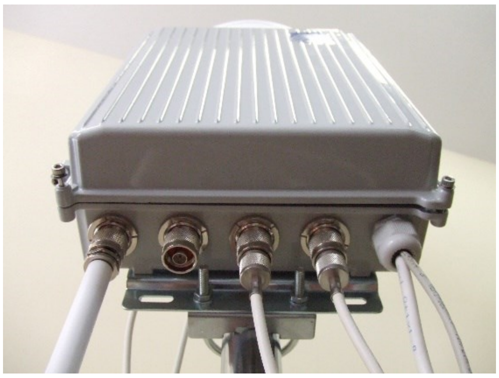
Q-Net consists of a central access point (AP) that is connected to multiple peripheral Subscriber Units (SUs). Any transmission of data that originates from the central AP is received by all of the peripheral CEs while any transmission of data that originates from any of the peripheral SUs is only received by the central AP. This equipment features improved transmission flexibility, lower operating costs and greater scope for service differentiation for the user. Point-to-multipoint microwave transmission system can be used for both mobile and DSL backhaul, because of the flexibility and cost control it provides. The network populated by hundreds of APs and SUs can be deployed quickly and expanded or moved easily as needs change. The system can be used as a backbone for several functional subsystems including video surveillance, traffic control and face recognition modules.

Q-Net components

Q-Net network consists of two major elements: Base Station and the CPE (Subscriber Unit). The Base Station (Picture 1) in standard configuration supports 4 sectors with 4 independent transceivers connected to external flat panel or omni antennas.



Subscriber Units are located within the coverage area of each BS sector and are managed by the BS. The Subscriber Unit includes one transceiver and integrated 14 dBi antenna (Picture 2).

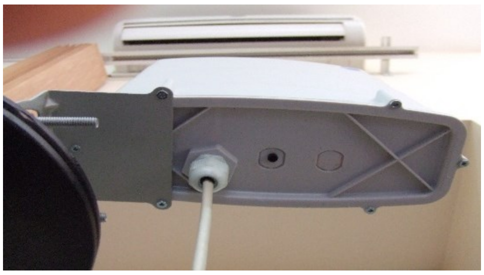


Picture 1

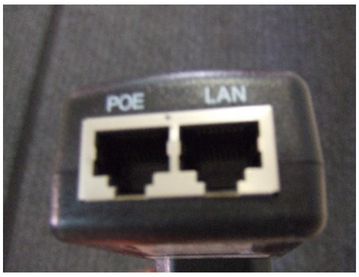
Picture 2

1. Interfaces

Bottom part of the Q-Net BS has 4 N-type antenna connectors and a separate cable inlet for power supply cable and 10/100 Base-T Ethernet cable (Picture 1)



Picture 3



Picture 4

Bottom part of the SU has a factory setting reset button (in the middle) and Ethernet cable inlet (Picture 3). The power supply for the SU is performed using POE (Power over Ethernet) technology, by a separate POE module included into the delivery (Picture 4)

Switching on

Prior to activation Q-Net Base Stations or Subscriber Units, the following steps are to be taken:

1. A proper location for BS or CPE needs to be selected, preferably with the direct line of sight towards the nearest site sector.

2. Interconnect BS (RJ-45 cable) with the core network through Ethernet switch, computer or other active network equipment.

3. Interconnect the unit with AC~220 V power supply.

4. When interconnecting the Subscriber Unit please make sure RJ-45 is connected to power injector (POE) and LAN cable is connected to the IP camera, PC or any other active network equipment.

5. Plug POE injector into the mains power supply.

Important! Before setting the BS or SU units into operational mode please make sure a) the IP address assigned to the device has no conflicts with other IP addresses in the WLAN and b) that the WLAN does not host any active DHCP server assigning IP addresses to network clients. In case one of these conditions are not observed, please follow instructions described below. You will need a laptop or PC interconnected with Q-Net BS or SU units LAN port.

Default settings for BS and SU unit:

LAN IP: 192.168.1.20

User name (login): **prox**

Password: **prox**

4. Unit configuration

Step I. Connect the BS to AC~ 220V mains power supply.

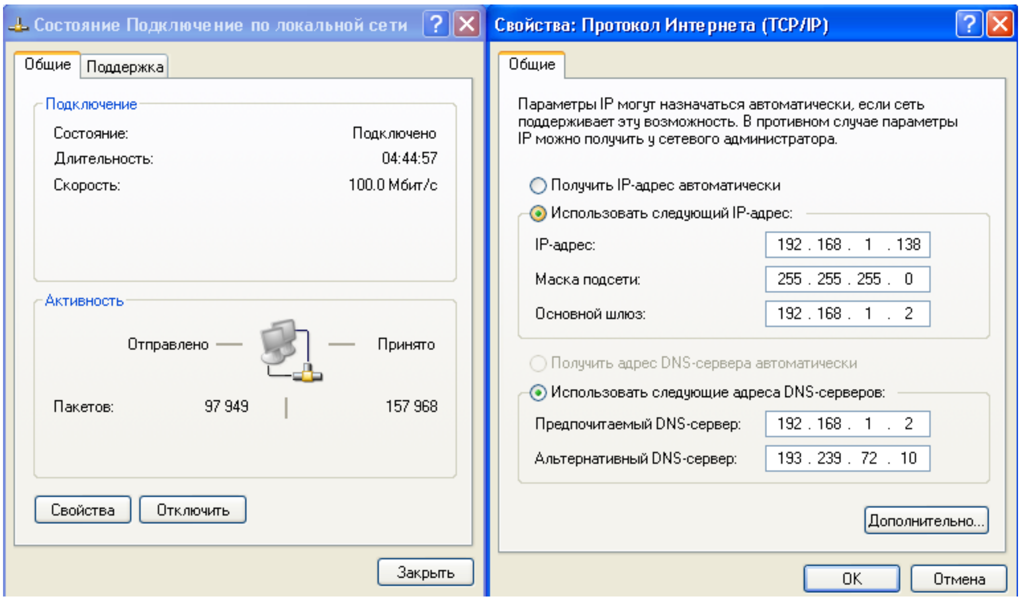
Step II. Wait till the BS is ready for operation (30-60 seconds)

Step III. Interconnect the PC or laptop with the BS . Ethernet card of the computer has to be assigned an IP address (any within the range 192.168.1.0~254 , for ex. 192.168.1.2) and subnet mask (255.255.255.0)

IMPORTANT! Factory default settings for BS transceivers (from left to right) are as follows:

Sector 1 transceiver	Sector 2 transceiver	Sector 3 transceiver	Sector 4 transceiver
LAN IP: 192.168.1.21	LAN IP: 192.168.1.22	LAN IP: 192.168.1.23	LAN IP: 192.168.1.24
Mask: 255.255.255.0	Mask: 255.255.255.0	Mask: 255.255.255.0	Mask: 255.255.255.0

In order to setup your IP address according to your nwetwork environment, please refer to **Network** section of this manual


Состояние Подключение по локальной сети
Общие
Поддержка
Свойства
Отключить
Закрыть
Свойства: Протокол Интернета (TCP/IP)
Общие
Дополнительно...
OK
Отмена

Подключение

Состояние: Подключено

Длительность: 04:44:57

Скорость: 100.0 Мбит/с

Активность

Отправлено — Принято

Пакетов: 97 949 | 157 968

Параметры IP могут назначаться автоматически, если сеть поддерживает эту возможность. В противном случае параметры IP можно получить у сетевого администратора.

○ Получить IP-адрес автоматически

● Использовать следующий IP-адрес:

IP-адрес: 192 . 168 . 1 . 138

Маска подсети: 255 . 255 . 255 . 0

Основной шлюз: 192 . 168 . 1 . 2

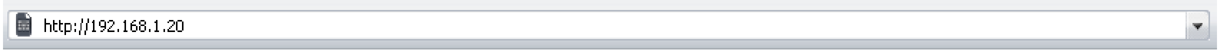
○ Получить адрес DNS-сервера автоматически

● Использовать следующие адреса DNS-серверов:

Предпочитаемый DNS-сервер: 192 . 168 . 1 . 2

Альтернативный DNS-сервер: 193 . 239 . 72 . 10

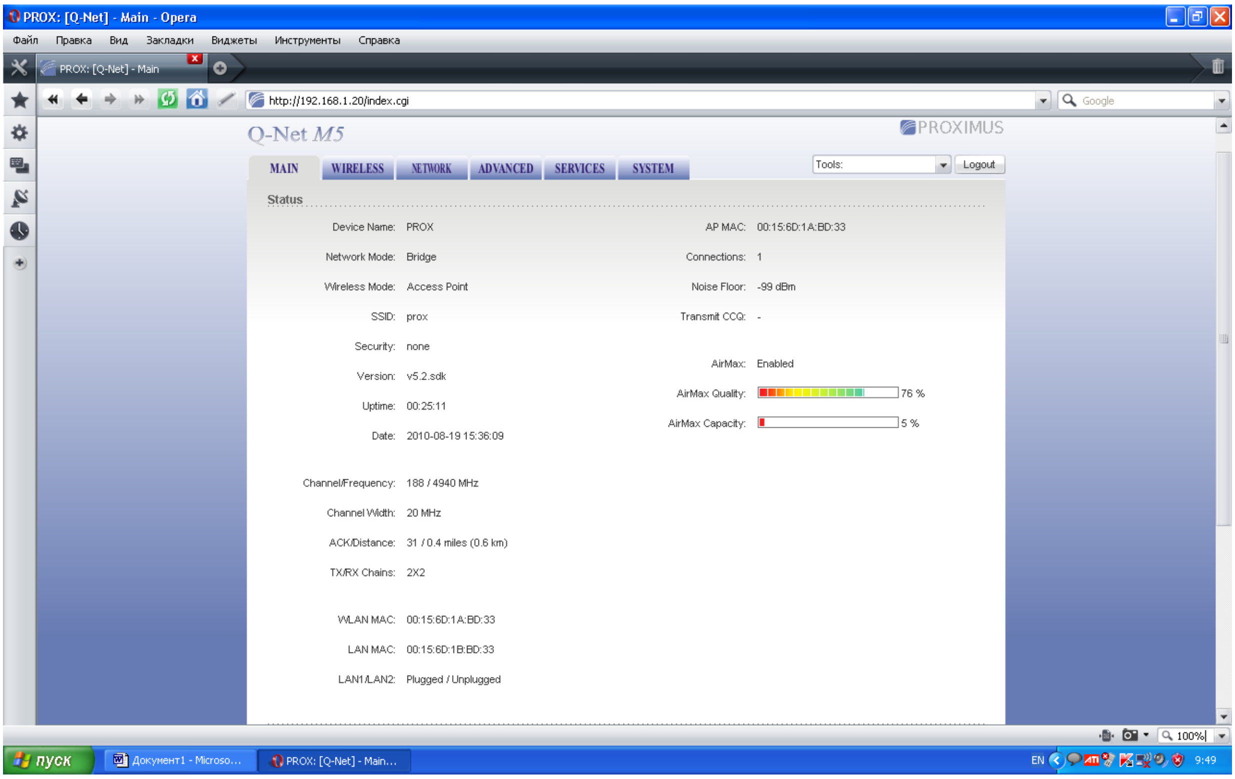
Step IV. As soon as your laptop or PC is switched to new settings, please run you Web browser and go to relevant IP address, for ex., http://192.168.1.21, which is the IP address for Transceiver 1 and press Enter.



http://192.168.1.20

Step V. In the new window that should apper, please ented you login and password and press Enter

Step VI. New web page that will appear on your screen contains 6 folders: Main, Wirelles, Network, Advanced, Services, System.(see screenshot below).



http://192.168.1.20/index.cgi

Status

Device Name: PROX

Network Mode: Bridge

Wireless Mode: Access Point

SSID: prox

Security: none

Version: v5.2.sdk

Uptime: 00:25:11

Date: 2010-08-19 15:36:09

Channel/Frequency: 188 / 4940 MHz

Channel Width: 20 MHz

ACK/Distance: 31 / 0.4 miles (0.6 km)

TX/RX Chains: 2X2

WLAN MAC: 00:15:6D:1A:BD:33

LAN MAC: 00:15:6D:1B:BD:33

LAN1/LAN2: Plugged / Unplugged

AP MAC: 00:15:6D:1A:BD:33

Connections: 1

Noise Floor: -99 dBm

Transmit CCQ: -

AirMax: Enabled

AirMax Quality: 76 %

AirMax Capacity: 5 %

4.1 Page “Main”

Pages	Parameters
Main	Page displays current status of the device and the statistical information. There are useful network administration and monitoring tools available in Main page also (i.e. antenna alignment tool, speed test utility, site survey tool while operating in AP mode
Wirelles	Page contains the controls for a wireless network configuration, while covering basic wireless settings which define operating mode, output power, associating details and data security options.
Network	Page covers the configuration of network operating mode, IP settings, packet filtering routines and network services
Advanced	Page settings are dedicated for more precise wireless interface control. It also includes antenna polarity, traffic shaping and QoS settings.
Services	Page covers the configuration of system management services (i.e. SNMP, NTP, System Log, Ping Watchdog and SSH/Telnet server).
System	Page contains controls for system maintenance routines, administrator account management, device customization, interface language, firmware upgrade and configuration backup

Main Page

displays a summary of link status information, current values of basic configuration settings (depending on operating mode), network settings and traffic statistics of all the interfaces. Network administration and monitoring utilities such as antenna alignment tool, ping and traceroute utilities, speed test tools are accessible via Main page also.

Device Name

Displays the customizable name (ID) of the Q-Net M5 based device. Device Name (Host Name) will be represented in registration screens of the Router Operating Systems and discovery tools.

Wirelles Mode

Displays the radio interface operating mode. Q-Net M5 powered device supports infrastructure wireless networking solution. Access Point (or Access Point WDS) and Station (or Station WDS) operating modes can be set depending on the network topology requirements.

Base Station SSID

SSID is the name of a wireless local area network (WLAN). All wireless devices on a WLAN must employ the same SSID in order to communicate with each other.

Security

This is the current security setting. “None” value is displayed if wireless security is disabled, WEP, WPA or WPA2 value is displayed if the corresponding wireless security method is used. More information is provided in the Link Setup section.

Uptime

This is the running total of time the device has been running since last power up (hard-reboot) or software upgrade. The time is expressed in days, hours, minutes and seconds.

Date

indicates the current system date and time, expressed in the form "year-month-day hours:minutes:seconds". Accurate system date and time is retrieved from the Internet services using NTP (Network Time Protocol). System date and time will be set to inaccurate default values after each reboot cycle if NTP is not enabled as most of the Q-Net M5 based devices have no autonomous power supply for the internal clock.

Channel / Frequency

This is the operating frequency. Device uses this frequency to transmit and receive data.

Channel Width

This is spectral width of the radio channel used by Q-Net M5 powered device. 5, 10, 20 and 40 MHz channel spectrum widths are supported. In Station (or Station WDS) 20/40MHz is the value by default.

ACK Timeout

Displays the current timeout value for ACK frames. ACK Timeout can be set manually or self-adjusted automatically. The ACK Timeout (Acknowledgement frame Timeout) specifies how long the Q-Net M5 device should wait for an acknowledgement from partner device confirming packet reception before concluding the packet must have been in error and requires resending. ACK Timeout is very important outdoor wireless performance parameter. When you are using 802.11n mode, it is recommended to set "Auto adjust" for ACK Timeout. More information is provided in the Advanced settings section.

TX/RX Chains

Displays the number of independent spatial data streams Q-Net M5 powered device is transmitting/receiving simultaneously within one spectral channel of bandwidth. This ability is specific for 802.11n devices which rely on multiple-input multiple-output (MIMO) technology. Multiple chains increase data transfer performance significantly.

WLAN MAC

Displays the MAC address of the Q-Net M5 device WLAN (Wireless) interface.

LAN MAC

Displays the MAC address of the Q-Net M5 device LAN (Ethernet) interface.

AP MAC

Displays the MAC address of the Access Point where the device has associated while operating in Station mode (or Station WDS). It is the MAC address of the Q-Net M5 powered device's wireless interface itself if operating in Access Point mode. AP MAC is used as Basic Service Set Identifier (BSSID) in infrastructure type wireless networks.

Connections

Displays the number of associated wireless stations while the device is operating in Access Point mode. This value is not displayed while operating in Station mode.

Noise Floor

Displays the current value of the noise level in dBm. Noise Floor is taken into account while evaluating the signal quality (Signal-to-Noise Ratio SNR, RSSI) while value mean depends on signal strength above the noise floor.

Transmit CCQ

This is an index of which evaluates the wireless Client Connection Quality. The level is based on a percentage value where 100% corresponds to a perfect link state.

Airmax

Indicates the current status of the AirMax in the device while operating in AP or AP WDS mode. If AirMax is enabled, the device only accepts AirMax stations. (Disable AirMax for legacy 802.11abg devices compatibility). AirMax also features some advanced QOS AutoDetection settings.

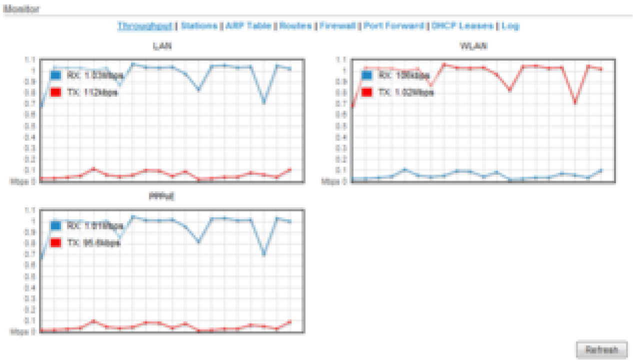
Airmax quality

This is an index which evaluates the AirMax Connection Quality. The level is based on a percentage value where 100% corresponds to a perfect link state.

Airmax Capacity

This is an index of maximum data rate the link is operating at. A Lower Capacity number indicates a unit that is bogging the system down.

Monitor



Throughput

Show graphs which continuously represents the current data traffic on the LAN, WLAN and PPP interfaces in both graphical and numerical form. The chart scale and throughput dimension (Bps, Kbps, Mbps) changes dynamically according to the mean throughput value. The statistics is updated automatically. Throughput statistics can be updated manually using the Refresh button.

Stations

This selection lists the stations which are connected to the device while operating in Access Point mode (or Access Point WDS).

The following statistics for every station associated is represented in the station statistics window:

Station MAC of the station which is associated;

Signal (dBm) value represents the last received wireless signal level;

Noise (dBm) value displays the value of the noise level wireless signal was received;

Tx Rate (Mbps) value represents the data rates, in Mbps, of the last transmitted packets;

Rx Rate (Mbps) value represents the data rates, in Mbps, of the last received packets;

Idle (sec) value represents the time (in seconds) since last packet was received from the particular station.

The information in the station statistics window can be updated using the Refresh button.

Station info

Detailed information can be retrieved while selecting the particular MAC of the associated station:

Connection time value represents the running total of time the station is associated. The time is expressed in days, hours, minutes and seconds;

Signal Strength value represents, in dBm, the last received wireless signal level;

Noise Floor: displays the current value of the noise level in dBm. Noise Floor is taken into account while evaluating the signal quality (Signal-to-Noise Ratio SNR, RSSI) while value mean depends on signal strength above the noise floor.

CCQ value represents the quality of the connection to the Station;

Tx/Rx Rate represents the data rates, in Mbps, of the last transmitted and received packets;

Tx/Rx Packets value represents the total amount of packets transmitted to and received from the Station during the connection uptime;

Tx/Rx Packet Rate (packets per second or pps) represents the mean value of the transmitted and received packet rate;

Bytes transmitted value represents the total amount of data (in bytes) transmitted during the connection;

Bytes received value represents the total amount of data (in bytes) received during the connection;

Negotiated Rate/Last Signal (dBm) table values represent the received wireless signal level along with the all data rates of recently received packets. “N/A” value is represented as the Last Signal if no packets were received on that particular data rate.

The information in the statistic window is updated automatically. The information in the station statistics window can be updated using the Refresh button. Window can be closed with the Close this window button.

AP Information

Selection opens the connection statistics window while operating in Station mode.

The following link statistics is provided:

MAC of the Access Point station is associated to;

Uptime value represents the running total of time the stations is associated to the AP. The time is expressed in days, hours, minutes and seconds;

Signal Strength value represents the last received wireless signal level;

CCQ value represents the quality of the connection to the AP;

Tx/Rx Rate represents the data rates of the last transmitted and received packets;

Tx/Rx Packets value represents the total amount of packets transmitted and received during the connection;

Tx/Rx Packet Rate (packets per second) represents the mean value of the transmitted and received packet rate;

Bytes transmitted/received value represents the total amount of data (in bytes) transmitted and received during the connection;

Negotiated Rate/Last Signal (dBm) table values represent the received wireless signal level along with the all data rates of recently received packets. "N/A" value is represented as the Last Signal if no packets were received on that particular data rate.

ARP Table

Selection lists all the entries of the ARP (Address Resolution Protocol) table currently recorded on the device.

The list can be updated using the Refresh button.

ARP is used to associate each IP address to the unique hardware address (MAC) the devices. It is important to have unique IP addresses for each MAC or else there will be ambiguous routes in the network.

Bridge

Selection lists all the entries in the system bridge table, while the device is operating in Bridge mode.

The list can be updated using the Refresh button.

Bridge table shows to which bridge port the particular station is associated to - in other words from which interface (Ethernet or wireless) the network device (defined by MAC address) is reachable to Q-Net M5 system while forwarding the packets to that port only (thus saving a lot of redundant copies and transmits).

Ageing timer shows ageing time for each address entry (in seconds) - after particular time out, not having seen a packet coming from a certain address, the bridge will delete that address from the Bridge Table.

Routes

Selection lists all the entries in the system routing table, while the device is operating in Router mode.

The list can be updated using the Refresh button.

Q-Net M5 examines the destination IP address of each data packet traveling through the system and chooses the appropriate interface to forward the packet to. The system choice depends on static routing rules – entries, which are registered in system routing table. Static routes to specific hosts, networks or default gateway are set up automatically according to the IP configuration of all the Q-Net M5 interfaces.

Q-Net M5 IP configuration description is provided in the Wireless section.

Firewall

Selection lists active firewall entries in the FIREWALL chain of the standard ebtables filter table, while the device is operating in Bridge mode.

The list can be updated using the 'Refresh button.

Active firewall entries in the FIREWALL chain of the standard iptables filter table are listed if the device is operating in Router mode.

The list can be updated using the Refresh button.

IP and MAC level access control and packet filtering in Q-Net M5 is implemented using iptables (routing) and ebtables (bridging) firewall which protects the resources of a private network from outside threats by preventing unauthorized access and filtering specified types of network communication.

More information is provided in the Wireless section.

Port Forward

Selection lists active port forward entries in the PORTFORWARD chain of the standard iptables nat table, while the device is operating in Router mode.

The list can be updated using the Refresh button.

Port Forwarding creates a transparent tunnel through a firewall/NAT, granting an access from the WAN side to the particular network service running on the LAN side.

DHCP Leases

Selection shows the current status of the leased IP addresses by the device's DHCP server. This option is available if DHCP Server is enabled while the device is operating in Router mode.

MAC address shows the client's MAC address, which is connected to the Access Point.

IP address shows the client's IP address leased by the device's DHCP server.

Remaining Lease time shows for how long the leased IP address will be valid and reserved for particular DHCP client.

Interface name shows from which device interface DHCP client which has specified MAC *Address* is connected.

The list can be updated using the Refresh button.

More information is provided in the Wireless section.

Log selection

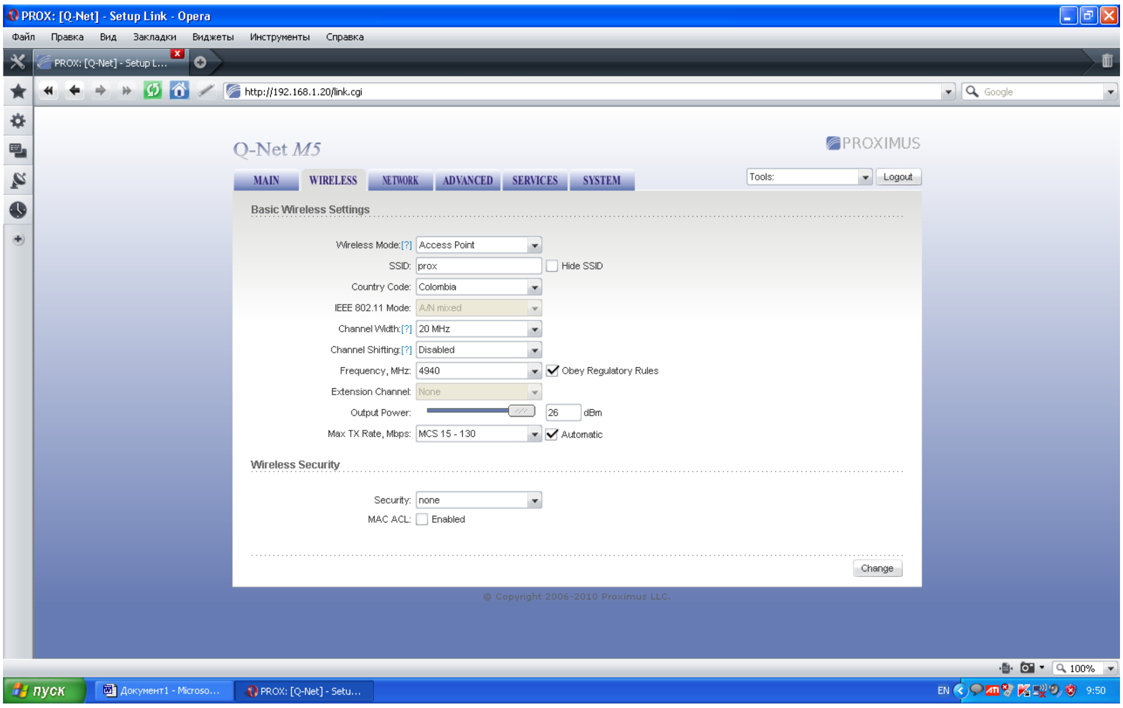
Shows a lists with all the registered system events.

All the entries in the system log will be deleted if the Clear button is activated. The System Log content is updated if Refresh button is activated.

Message "Syslog is disabled, unable to show system messages" is displayed if the System Log is not enabled. System Log configuration description is provided in the Services section.

Page "Wirelles"

The Wirelles Page contains everything needed by the operator to setup the wireless part of the link. This includes regulatory requirements, channel and frequency settings, device mode, data rates, and wireless security.


PROX: [Q-Net] - Setup Link - Opera
Файл Правка Вид Закладки Виджеты Инструменты Справка
PROX: [Q-Net] - Setup L...
http://192.168.1.20/link.cgi
Google
Q-Net M5
PROXIMUS
MAIN
WIRELESS
NETWORK
ADVANCED
SERVICES
SYSTEM
Tools:
Logout
© Copyright 2006-2010 Proximus LLC.
100%
пуск
Документ1 - Microso...
PROX: [Q-Net] - Setu...
EN
9:50

Basic Wireless Settings

Wireless Mode:[?] Access Point
SSID: prox ☐ Hide SSID
Country Code: Colombia
IEEE 802.11 Mode: A/N mixed
Channel Width:[?] 20 MHz
Channel Shifting:[?] Disabled
Frequency, MHz: 4940 ☑ Obey Regulatory Rules
Extension Channel: None
Output Power: 26 dBm
Max TX Rate, Mbps: MCS 15 - 130 ☑ Automatic

Wireless Security

Security: none
MAC ACL: ☐ Enabled

Change

Wireless Mode

Specify the operating mode of the device. The mode depends on the network topology requirements. There are 4 operating modes supported in software:

1. ***Station:*** This is a client mode, which can connect to an AP.

   It is common for a bridging application to an AP. In Station mode device acts as the Subscriber Station while connecting to the Access Point which is primary defined by the SSID and forwarding all the traffic to/from the network devices connected to the Ethernet interface.

   The specifics of this mode is that Subscriber Station is using arpnat technique which may result lack of transparency while passing-through broadcast packets in bridge mode.

2. ***Station WDS:*** WDS stands for Wireless Distribution System. Station WDS should be used while connecting to the Access Point which is operating in WDS mode. This mode is compatible with WPA/WPA2 encryption.

   Station WDS mode enables packet forwarding at layer 2 level.

   The benefit of Station WDS is improved performance and faster throughput. Station WDS - Bridge mode is fully transparent for all the Layer2 protocols.

   Refer to the section Network Settings for detailed Bridge network mode configuration information.

3. ***Access Point:*** This is an 802.11 Access Point

4. ***Access Point WDS:*** This is an 802.11 Access Point which allows for layer 2 bridging with Station WDS devices using the WDS protocol. AP WDS is not fully compatible with WPA/WPA2 encryption.

   WDS allows you to bridge wireless traffic between devices which are operating in Access Point mode. Access Point is usually connected to a wired network (Ethernet LAN) allowing wireless connection to the wired network. By connecting Access Points to one another in an Extended Service Set using the WDS, distant Ethernets can be bridged into a single LAN.

   It is important that network loops should not be created with either WDS bridges or combinations of wired (Ethernet) connections and WDS bridges. Tree or Star shape network topology should be used in all WDS use-cases (i.e. if AP2 and AP3 are specified as the WDS peers of AP1, AP2 should not be specified as the WDS peer of AP3 and AP3 should not be specified as the WDS peer of AP2 in any case). Mesh and Ring network topologies are not supported by WDS and should be avoided in all the use cases.

Note: Station WDS and AP WDS mode uses the WDS protocol which is not defined as the standard thus compatibility issues between equipment from different vendors may arise.

WDS Peers: WDS Stations and/or WDS Access Points connected to the Access Point should be specified in this list in order to create a wireless network infrastructure - Wireless Distribution System (applicable for AP WDS mode only).

Enter the MAC address of the paired WDS device in the WDS Peer entry field. One MAC address should be specified for Point-to-Point connection use case, up to six WDS Peers can be specified for Point-to-Multi-Point connection use case.

Auto option should be enabled in order to establish WDS connection between Access Points if WDS Peers are not specified (applicable for AP WDS mode only). If Auto option is enabled Access Point will choose WDS Peers (Access Points) according to the SSID setting. Access Point operating in WDS mode should have the same SSID as the WDS Peer in order to establish the connection automatically while Auto option is enabled. This configuration is also known as the repeater mode. AP WDS Auto option can not be selected if any type of WPA or WPA2 security is used as WPA requires different roles on AP configuration (authenticator or supplicant).

Note: Access Point operating in WDS mode and all the WDS Peers must operate on the same frequency channel and use the same channel spectrum width.

SSID: Service Set Identifier used to identify wireless LAN should be specified while operating in Access Point mode. All the client devices within range will receive broadcast messages from the access point advertising this SSID.

Hide SSID: Control will disable advertising the SSID of the access point in broadcast messages to wireless stations. Unselected control will make SSID visible during network scans on the wireless stations. Control is available while operating in Access Point mode only.

ESSID: specify the ESSID of the Access Point which the Q-Net M5 should associate to while operating in Station or Station WDS mode. There can be several Access Points with the same ESSID. If the ESSID is set to “Any” the station will connect to any available AP.

The list of the available Access Points can be retrieved using the Select button (not applicable to Access Point mode). This control activates Site Survey tool which is used for the AP selection. Site Survey will search for the available wireless networks in range on all the supported channels and will allow you to select one for association. In case the selected network uses encryption, you’ll need to set security parameters in Wireless Security section. Select the Access Point from the list and click Select button for association.

Click Scan button to refresh the list of available wireless networks. Site Survey channel scan list can be modified using the Channel Scan List control.

Lock to AP MAC: This allows the station to always maintain connection to a particular AP with a specific MAC (applicable for Station and Station WDS mode only). This is useful as sometimes there can be few identically named SSID's (AP's) with different MAC addresses. With AP lock on, the station will lock to MAC address and not roam between several Access Points with the same ESSID.

Country Code: Different countries will have different power levels and possible frequency selections. To ensure device operation follows regulatory compliance rules, please make sure to select your correct country where device will be used.

Channel Spectrum Width: This is spectral width of the radio channel. Supported wireless channel spectrum widths:

5MHz – is the channel spectrum with the width of 5 MHz (known as Quarter-Rate mode).

10MHz – is the channel spectrum with the width of 10 MHz (known as Half-Rate mode).

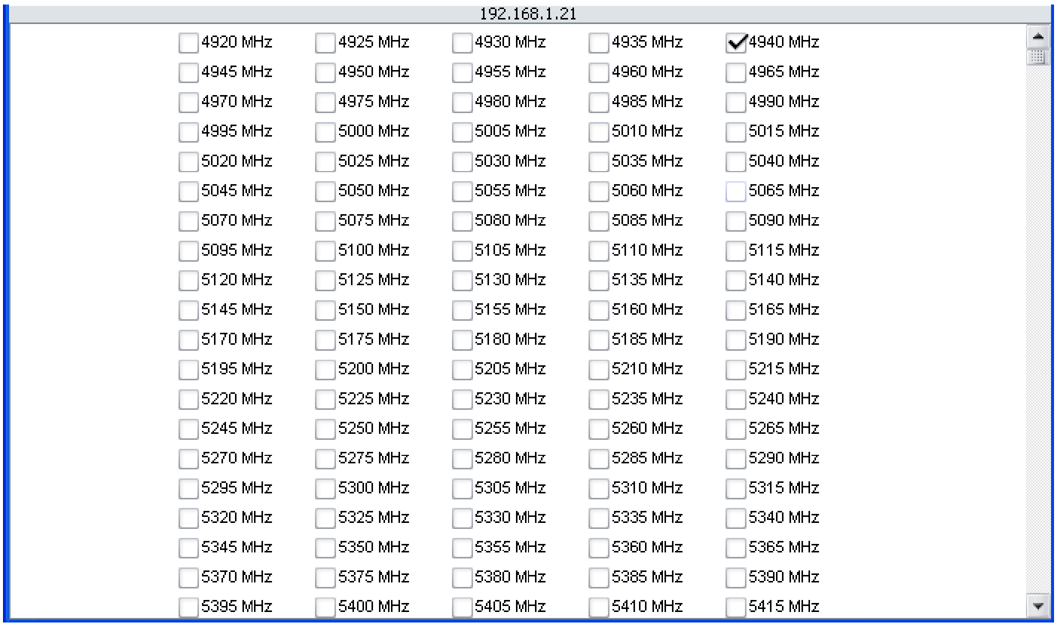
20MHz – is the standard channel spectrum width (selected by default).

40MHz – is the channel spectrum with the width of 40 MHz.

20MHz/40MHz – only available in Station (or Station WDS) mode. It offers better compatibility.

Channel Shifting: option enables the special channels which have the frequency offset. All the channels can be shifted by 2 MHz from the default central channel frequency.

Frequency, MHz: select the wireless channel while operating in Access Point mode. Multiple frequency channels are available to avoid interference between nearby access points. The channel list varies depending on the selected country code, IEEE 802.11 mode and Channel Spectrum Width and Channel Shifting option.



192.168.1.21

☐ 4920 MHz	☐ 4925 MHz	☐ 4930 MHz	☐ 4935 MHz	☑ 4940 MHz
☐ 4945 MHz	☐ 4950 MHz	☐ 4955 MHz	☐ 4960 MHz	☐ 4965 MHz
☐ 4970 MHz	☐ 4975 MHz	☐ 4980 MHz	☐ 4985 MHz	☐ 4990 MHz
☐ 4995 MHz	☐ 5000 MHz	☐ 5005 MHz	☐ 5010 MHz	☐ 5015 MHz
☐ 5020 MHz	☐ 5025 MHz	☐ 5030 MHz	☐ 5035 MHz	☐ 5040 MHz
☐ 5045 MHz	☐ 5050 MHz	☐ 5055 MHz	☐ 5060 MHz	☐ 5065 MHz
☐ 5070 MHz	☐ 5075 MHz	☐ 5080 MHz	☐ 5085 MHz	☐ 5090 MHz
☐ 5095 MHz	☐ 5100 MHz	☐ 5105 MHz	☐ 5110 MHz	☐ 5115 MHz
☐ 5120 MHz	☐ 5125 MHz	☐ 5130 MHz	☐ 5135 MHz	☐ 5140 MHz
☐ 5145 MHz	☐ 5150 MHz	☐ 5155 MHz	☐ 5160 MHz	☐ 5165 MHz
☐ 5170 MHz	☐ 5175 MHz	☐ 5180 MHz	☐ 5185 MHz	☐ 5190 MHz
☐ 5195 MHz	☐ 5200 MHz	☐ 5205 MHz	☐ 5210 MHz	☐ 5215 MHz
☐ 5220 MHz	☐ 5225 MHz	☐ 5230 MHz	☐ 5235 MHz	☐ 5240 MHz
☐ 5245 MHz	☐ 5250 MHz	☐ 5255 MHz	☐ 5260 MHz	☐ 5265 MHz
☐ 5270 MHz	☐ 5275 MHz	☐ 5280 MHz	☐ 5285 MHz	☐ 5290 MHz
☐ 5295 MHz	☐ 5300 MHz	☐ 5305 MHz	☐ 5310 MHz	☐ 5315 MHz
☐ 5320 MHz	☐ 5325 MHz	☐ 5330 MHz	☐ 5335 MHz	☐ 5340 MHz
☐ 5345 MHz	☐ 5350 MHz	☐ 5355 MHz	☐ 5360 MHz	☐ 5365 MHz
☐ 5370 MHz	☐ 5375 MHz	☐ 5380 MHz	☐ 5385 MHz	☐ 5390 MHz
☐ 5395 MHz	☐ 5400 MHz	☐ 5405 MHz	☐ 5410 MHz	☐ 5415 MHz

Output Power: This will configure the maximum average transmit output power (in dBm) of the wireless device. The output power at which wireless module transmits data can be specified using the slider. When entering output power value manually, the slider position will change according to the entered value.

Obey regulatory power option must remain enabled while it will force the transmit output power to be compliant with the regulations of the selected country.

Data Rate: This defines the data rate (in Mbps) at which the device should transmit wireless packets. If the Best (automatic) option is selected, then the rate algorithm will select the best data rate depending on the link quality conditions. You can fix a specific data rate between MCS 0 and MCS 7 (or MCS15 for 2x2 chains devices) also. Use Best (automatic) option if you are having trouble getting connected or losing data at a higher rate. In this case the lower data rates will be used by device automatically. If you select 20MHz Channel Spectrum width the maximum data rate is MCS7 (65Mbps) or MCS15 (150Mbps). If you select 40MHz Channel Spectrum width the maximum data rate is MCS7 (150Mbps) or MCS15 (300Mbps).

Wireless Security

This section enables you to set parameters that control how the subscriber station associates to a wireless device and encrypts/decrypts data.

Wireless Security Settings

Choose the security method according to the Access Point security policy. Subscriber station should be authorized by Access Point in order to get access to the network and all the user data transferred between subscriber station and Access Point will be encrypted if the wireless security methods are used.

Security. Q-net supports WEP, WPA, and WPA2 security options. Select the security mode of your wireless network:

WEP – enable WEP encryption. WEP (Wired Equivalent Privacy) uses the RC4 encryption algorithm. Enabling WEP allows you to increase security by encrypting data being transferred over your wireless network. WEP is the oldest security algorithm, and there are few applications that can decrypt the WEP key in less than 10 minutes. WPA/WPA2 security methods should be used when possible.

WPA – enable WPA security mode. WPA and WPA2 with pre-shared key management protocol offers improved security methods. WPA and WPA2 support the following ciphers for data encryption:

TKIP - Temporal Key Integrity Protocol which uses RC4 encryption algorithm.

CCMP (commonly known as AES) - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol which uses the Advanced Encryption Standard (AES) algorithm.

The device will use the strongest cipher (CCMP) in Station and Access Point wireless mode by default. If CCMP is not supported on the other side of the link the TKIP encryption will be used - like in situation when the device acts as Access Point with WPA security enabled and at least one wireless station (without CCMP support) is connected to it.

WPA – enable WPA security mode.

WPA-TKIP – enable WPA security mode with TKIP support only.

WPA-AES – enable WPA security mode with AES support only.

WPA2 – enable WPA2 security mode.

WPA2-TKIP – enable WPA2 security mode with TKIP support only.

WPA2-AES – enable WPA2 security mode with AES support only.

WEP security

Authentication Type: field relates only to the WEP security option. One of the following authentication modes should be selected if WEP security method is used:

Open Authentication – station is authenticated automatically by AP (selected by default).

Shared Authentication – station is authenticated after the challenge, generated by AP.

WEP Key Length: 64-bit (selected by default) or 128-bit WEP Key length should be selected if WEP security method is used. The 128-bit option will provide a bit higher level of wireless security.

Key Type: HEX (selected by default) or ASCII option specifies the character format for the WEP key if WEP security method is used.

WEP Key: WEP encryption key for the wireless traffic encryption and decryption should be specified if WEP security method is used:

For 64-bit – specify WEP key as 10 HEX (0-9, A-F or a-f) characters (e.g. 00112233AA) or 5 ASCII characters.

For 128-bit – specify WEP key as 26 HEX (0-9, A-F or a-f) characters (e.g. 00112233445566778899AABBCC) or 13 ASCII characters.

Key Index: allows to specify the Index of the WEP Key used. 4 different WEP keys can be configured at the same time, but only one is used. Effective key is set with a choice of 1, 2, 3 or 4.

WPA/WPA2 PSK security

WPA Authentication: one of the following WPA™ key selection methods should be specified if WPA™ or WPA2™ security method is used (applicable for Station and Station WDS modes only). :

PSK – WPA or WPA2 with Pre-shared Key method (selected by default).

EAP – WPA or WPA2 with EAP (Extensible Authentication Protocol) authentication method. This method is commonly used in Enterprise networks.

WPA Pre-shared Key: the pass phrase for WPA or WPA2 security method should be specified if the Pre-shared Key method is selected. The pre-shared key is an alpha-numeric password between 8 and 63 characters long.

WPA/WPA2 EAP security

WPA Identity: identification credential (also known as identity) used by the supplicant for EAP authentication (applicable for STA and STA WDS modes only).

WPA User Name: identification credential (also known as anonymous identity) used by the supplicant for EAP tunneled authentication (EAP-TTLS) in unencrypted form (applicable for STA and STA WDS modes only).

WPA User Password: password credential used by the supplicant for EAP authentication (applicable for STA and STA WDS modes only).

MAC ACL: MAC Access Control List (ACL) provides ability to allow or deny certain clients to connect to the AP (applicable for AP and AP WDS modes only).

MAC ACL can be enabled by selecting the Enabled option.

There are two ways to set the Access Control List:

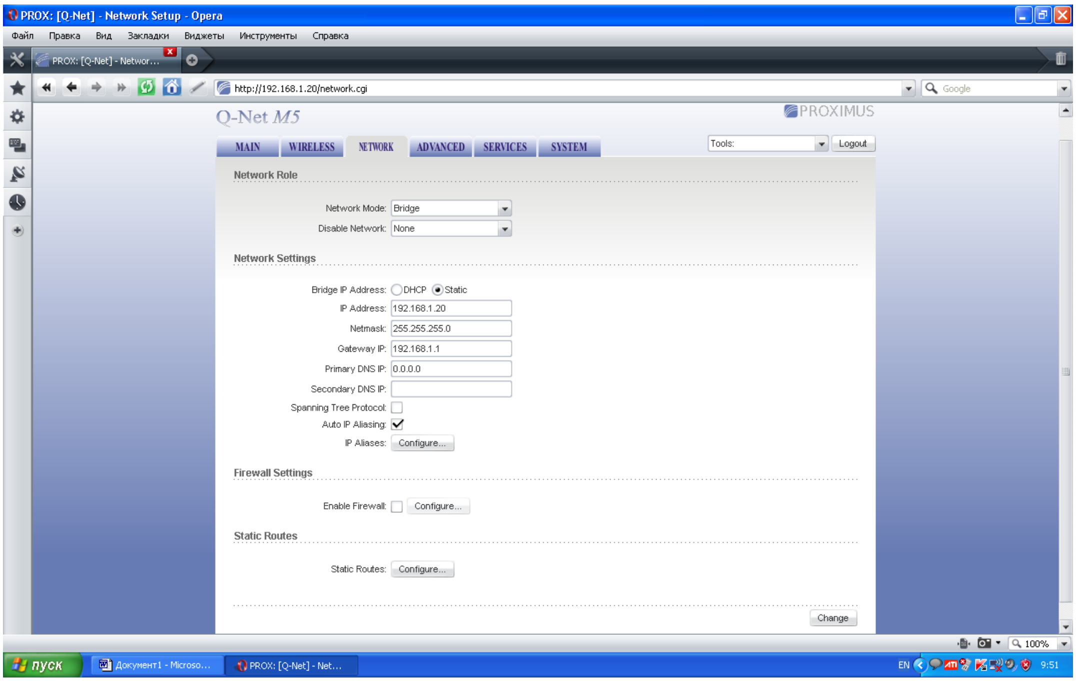
- define certain wireless clients in the list which will have granted access to the Access Point while the access will be denied for all the remaining clients - MAC ACL Policy is set to Allow'.

- define certain wireless clients in the list which will have denied access to the Access Point while the access will be granted for all the remaining clients - MAC ACL Policy is set to Deny.

The MAC addresses of the wireless clients can be added and removed to the list using the Add and Remove buttons.

Click ***Change button*** to save the changes.

Page "Network"


PROX: [Q-Net] - Network Setup - Opera
Файл Правка Вид Закладки Виджеты Инструменты Справка
http://192.168.1.20/network.cgi
Q-Net M5
PROXIMUS
MAIN
WIRELESS
NETWORK
ADVANCED
SERVICES
SYSTEM
Tools:
Logout
пуск
PROX: [Q-Net] - Net...

Network Role

Network Mode: Bridge

Disable Network: None

Network Settings

Bridge IP Address: ○ DHCP ● Static

IP Address: 192.168.1.20

Netmask: 255.255.255.0

Gateway IP: 192.168.1.1

Primary DNS IP: 0.0.0.0

Secondary DNS IP:

Spanning Tree Protocol: □

Auto IP Aliasing: ☑

IP Aliases: Configure...

Firewall Settings

Enable Firewall: □ Configure...

Static Routes

Static Routes: Configure...

Change

The Network Page allows the administrator to setup bridge or routing functionality.

Q-net devices can operate in bridge or router mode. The IP configuration as described below is required for device management purposes. IP addresses can either be retrieved from a DHCP server or configured manually. Use the Network menu to configure the IP settings.

Network Mode: specify the operating network mode for the device. There are two modes: bridge and router.

The mode depends on the network topology requirements:

Bridge operating mode is selected by default as it is widely used by the subscriber stations, while connecting to Access Point or using WDS. In this mode the device will act as a transparent bridge and will operate in Layer 2. There will be no network segmentation while broadcast domain will be the same. Bridge mode will not block any broadcast or multicast traffic. Additional Firewall settings can be configured for Layer 2 packet filtering and access control in Bridge mode.

Router operating mode can be configured in order to operate in Layer 3 to perform routing and enable network segmentation – wireless clients will be on different IP subnet. Router mode will block broadcasts while it is not transparent.

Q-net supports Multicast packet pass-through in Router mode.

Q-net Router can act as DHCP server and use Network Address Translation (Masquerading) feature which is widely used by the Access Points. NAT will act as the firewall between LAN and WLAN networks. Additional Firewall settings can be configured for Layer 3 packet filtering and access control in Router mode.

Disable Network: options can be used for disabling WLAN or LAN interface. This setting should be used with the exclusive care as no L2 or L3 connection can be established through the disabled interface. It will be impossible to access the device from the wireless/wired network which is connected to the disabled interface.

Bridge mode Network Settings

In bridge mode the device forwards all the network management and data packets from one network interface to the other without any intelligent routing. For simple applications this provides efficient and fully transparent network solution. WLAN (wireless) and LAN (Ethernet) interfaces belong to the same network segment which has the same IP address space. WLAN and LAN interfaces form the virtual bridge interface while acting as the bridge ports. The bridge has assigned IP settings for management purposes:

Bridge IP Address: The device can be set for static IP or can be set to obtain an IP address from the DHCP server it is connected to.

One of the IP assignment modes must be selected:

> DHCP – choose this option to assign the dynamic IP address, Gateway and DNS address by the local DHCP server.
>
> Static – choose this option to assign the static IP settings for the bridge interface.

IP Address: enter the IP address of the device while Static Bridge IP Address mode is selected. This IP will be used for the Q-Net device management purposes.

Bridge IP Address assigned manually (Static)

IP Address and Netmask settings should consist with the address space of the network segment where Q-Net device resides. If the device IP settings and administrator PC (which is connected to the device in wired or wireless way) IP settings will use different address space, the Q-Net device will become unreachable.

Netmask: This is a value which when expanded into binary provides a mapping to define which portions of IP address groups can be classified as host devices and network devices. Netmask defines the address space of the network segment where Q-Net device resides. 255.255.255.0 (or /24) Netmask is commonly used among many C Class IP networks.

Gateway IP: Typically, this is the IP address of the host router which provides the point of connection to the internet. This can be a DSL modem, Cable modem, or a WISP gateway router.

Device will direct the packets of data to the gateway if the destination host is not within the local network.

Gateway IP address should be from the same address space (on the same network segment) as the Q-Net device.

Primary/Secondary DNS IP: The Domain Name System (DNS) is an internet "phone book" which translates domain names to IP addresses. These fields identify the server IP addresses of where the Q-Net device looks for the translation source.

Primary DNS server IP address should be specified for the device management purposes.

Secondary DNS server IP address is optional. It is used as the fail-over in case the primary DNS server will become unresponsive.

DHCP Fallback IP: In case the Bridge is placed in Dynamic IP Address mode (DHCP) and is unable to obtain an IP address from a valid DHCP server, it will fall back to the static IP address listed here.

Q-Net system will return to the default IP configuration (192.168.1.20/255.255.255.0) If the Reset to defaults routine is initiated.

Spanning Tree Protocol: Multiple interconnected bridges create larger networks using the Spanning Tree Protocol (STP), which is used for finding the shortest path within network and to eliminate loops from the topology.

Spanning Tree Protocol enabled

If the STP is turned on, the Q-Net Bridge will communicate with other network devices by sending and receiving Bridge Protocol Data Units (BPDU). STP should be turned off (selected by default) when the Q-Net device is the only bridge on the LAN or when there are no loops in the topology as there is no sense for the bridge to participate in the Spanning Tree Protocol in this case.

Firewall functionality on bridge interface can be enabled using the "Enable Firewall" option. Bridge Firewall rules can be configured, enabled or disabled while using Firewall configuration window which is opened with the "Configure" button.

Bridge mode Firewall Configuration Settings

Firewall entries can be specified by using the following criteria:

Interface the interface (WLAN or LAN) where filtering of the incoming/passing-through packets is processed;

IP Type sets which particular L3 protocol type (IP, ICMP, TCP, UDP) should be filtered;

Source IP/mask is the source IP of the packet (specified within the packet header), usually it is the IP of the host system which sends the packets;

Source Port is the source port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application which sends the packets;

Destination IP/mask is the destination IP of the packet (specified within the packet header), usually it is the IP of the system which the packet is addressed to;

Destination Port is the destination port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application which the packet is addressed to.

Comments is the informal field for the comment of the particular firewall entry. Few words about the particular firewall entry purpose are saved there usually.

On flag enables or disables the effect of the particular firewall entry. All the added firewall entries are saved in system configuration file, however only the enabled firewall entries will be active during the Q-Net system operation.

Not operators can be used for inverting the Source IP/mask, Source Port, Destination IP/mask and Destination Port filtering criteria (i.e. if not is enabled for the specified Destination Port value 443, the filtering criteria will be applied to all the the packets sent to any Destination Port except the 443 which is commonly used by HTTPS).

Newly added Firewall entries can be saved by activating Save button or discarded by activating Cancel button in the Firewall configuration window.

All the active firewall entries are stored in the FIREWALL chain of the ebtables filter table, while the device is operating in Bridge mode. Please refer to the ebtables manual for detailed description of the firewall functionality in Bridge mode.

The list can be updated using the Reload button.

Click Change button to save the changes made in the Network page.

Router Mode

Network - Router mode

The role of the LAN and WLAN interface will change accordingly to the Wireless Mode while the Q-Net powered device is operating in Router mode:

- Wireless interface and all the wireless clients connected are considered as the internal LAN and the Ethernet interface is dedicated for the connection to the external network while the Q-Net powered device is operating in *AP/AP WDS* wireless mode;

- Wireless interface and all the wireless clients connected is considered as the external network and the all the network devices on LAN side as well as the Ethernet interface itself is considered as the internal network while the Q-Net powered device is operating in *Station/Station WDS* mode.

Wireless/wired clients are routed from the internal network to the external one by default. Network Address Translation (NAT) functionality works the same way.

WLAN Network Settings

IP Address**:** This is the IP addresses to be represented by the WLAN interface which is connected to the internal network according to the wireless operation mode described above. This IP will be used for the routing of the internal network (it will be the Gateway IP for all the devices connected on the internal network). This is the IP address can be used for the management purpose of the Q-Net powered device.

Auto IP Aliasing configures automatically generated IP Address for the corresponding WLAN/LAN interface if enabled. Generated IP address is the unique Class B IP address from the 169.254.X.Y range (Netmask 255.255.0.0) which are intended for use within the same network segment only.

Auto IP always starts with 169.254.X.Y while X and Y are last 2 digits from device MAC address (i.e. if the MAC is 00:15:6D:A3:04:FB, Generated unique Auto IP will be 169.254.4.251).

Netmask: This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical netmask value for Class C networks, which support IP address range 192.0.0.x to 223.255.255.x. Class C network Netmask uses 24 bits to identify the network (alternative notation "/24") and 8 bits to identity the host.

IP Aliases

IP Aliases for internal and external network interface can be configured. IP Aliases can be specified using the IP Aliases configuration window which is opened while activating the "Configure" button.

IP Address is the alternative IP address for the LAN or WLAN interface, which can be used for the routing or device management purposes;

Netmask is the network address space identifier for the particular IP Alias;

Comments is the informal field for the comment of the particular IP Alias. Few words about the alias purpose are saved there usually;

Enabled flag enables or disables the particular IP Alias. All the added IP Aliases are saved in system configuration file, however only the enabled IP Aliases will be active during the Q-Net system operation.

Newly added IP Aliases can be saved by activating Save button or discarded by activating Cancel button in the Aliases configuration window.

Enable NAT and DHCP Server

Enable NAT: Network Address Translation (NAT) enables packets to be sent from the wired network (LAN) to the wireless interface IP address and then sub-routed to other client devices residing on it's local network while the Q-Net powered device is operating in AP/AP WDS wireless mode and in the contrariwise direction in "Station/Station WDS" mode.

NAT is implemented using the masquerade type firewall rules. NAT firewall entries are stored in the iptables nat table, while the device is operating in Router mode. Please refer to the iptables tutorial for detailed description of the NAT functionality in Router mode.

Static routes should be specified in order the packets should pass-through the Q-Net based device if the NAT is disabled in while operating in Router network mode.

Enable DHCP Server: Dynamic Host Configuration Protocol (DHCP) Server assigns IP addresses to clients which will associate to the wireless interface while the Q-Net powered device is operating in AP/AP WDS wireless mode and assigns IP addresses to clients which will connect to the LAN interface while the Q-Net powered device is operating in Station/Station WDS mode.

DHCP Server range and lease time

Range Start/End: This range determines the IP addresses given out by the DHCP server to client devices on the internal network which use dynamic IP configuration.

Netmask: This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical netmask value for Class C networks, which support IP address range 192.0.0.x to 223.255.255.x. Class C network Netmask uses 24 bits to identify the network (alternative notation "/24") and 8 bits to identity the host.

Lease Time: The IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interrupt, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more slight interruptions to the client while it will acquire new IP addresses from the DHCP server.

DNS Proxy: The DNS Proxy forwards the Domain Name System requests from the hosts which reside in the internal network to the DNS server while Q-Net powered device is in operating in Router mode. Valid Primary DNS Server IP needs to be specified for DNS Proxy functionality. Internal network interface IP of the Q-Net powered device should be specified as the DNS server in the host configuration in order DNS Proxy should be able to get the DNS requests and translate domain names to IP addresses afterwards.

Port Forwarding: Port forwarding allows specific ports of the hosts residing in the internal network to be forwarded to the external network. This is useful for number of applications such as FTP servers, gaming, etc. where different host systems need to be seen using a single common IP address/port.

Port Forwarding rules can be set in Port Forwarding window, which is opened by enabling the Port Forwarding option and activating the Configure button.

Port Forwarding entries can be specified by using the following criteria:

Private IP is the IP of the host which is connected to the internal network and needs to be accessible from the external network;

Private Port is the TCP/UDP port of the application running on the host which is connected to the internal network. The specified port will be accessible from the external network;

Type is the L3 protocol (IP) type which need to be forwarded from the internal network.

Public Port is the TCP/UDP port of the Q-Net based device which will accept and forward the connections from the external network to the host connected to the internal network.

Comments is the informal field for the comment of the particular port forwarding entry. Few words about the particular port forwarding entry purpose are saved there usually.

Enabled flag enables or disables the effect of the particular port forwarding entry. All the added firewall entries are saved in system configuration file, however only the enabled port forwarding entries will be active during the Q-Net system operation.

Newly added port forwarding entries can be saved by activating Save button or discarded by activating Cancel button in the Port Forwarding configuration window.

LAN Network Settings

LAN IP Address: This is the IP addresses to be represented by the LAN or WLAN interface which is connected to the external network according to the wireless operation mode described above. This is the IP address can be used for the routing and the device management purposes.

The external network interface can be set for static IP or can be set to obtain an IP address from the DHCP server which should reside in the external network. One of the IP assignment modes must be selected for the external network interface:

DHCP – choose this option to obtain the IP address, Gateway and DNS address dynamically from the external DHCP server.

PPPoE – choose this option to obtain the IP address, Gateway and DNS address dynamically from the external PPPoE server.

Static – choose this option to assign the static IP settings for the external interface.

LAN IP Address assigned manually - Static

IP Address and Netmask settings should consist with the address space of the network segment where Q-Net device resides. If the device IP settings and administrator PC (which is connected to the device in wired or wireless way) IP settings will use different address space, the Q-Net device will become unreachable.

Netmask: This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical netmask value for Class C networks, which support IP address range 192.0.0.x to 223.255.255.x. Class C network Netmask uses 24 bits to identify the network (alternative notation "/24") and 8 bits to identity the host.

Gateway IP: is the IP address of the host router which resides on the external network and provides the point of connection to the next hop towards the internet. This can be a DSL modem, Cable modem, or a WISP gateway router. Q-Net device will direct all the packets to the gateway if the destination host is not within the local network.

Gateway IP address should be from the same address space (on the same network segment) as the Q-Net device's external network interface (Wireless interface in the Station case and the LAN interface in the AP case).

Primary/Secondary DNS IP: The Domain Name System (DNS) is an internet "phone book" which translates domain names to IP addresses. These fields identify the server IP addresses where the DNS requests are forwarded by the Q-Net powered device.

Primary DNS server IP is mandatory. It is used by the DNS Proxy and for the device management purpose.

Secondary DNS server IP address is optional. It is used as the fail-over in case the primary DNS server will become unresponsive.

PPPoE Internet connection (usually used by ADSL providers)

PPPoE: Point-to-Point Protocol over Ethernet (PPPoE) is a virtual private and secure connection between two systems which enables encapsulated data transport. It is commonly used as the medium for subscribers to connect to Internet Service Providers.

Select the IP Address option PPPoE to configure a PPPoE tunnel in order to connect to an ISP. Only the external network interface can be configured as PPPoE client as all the traffic will be sent via this tunnel. The IP address, Default gateway IP and DNS server IP address will be obtained from the PPPoE server after PPPoE connection is established. Broadcast address is used for the PPPoE server discovery and tunnel establishment.

Valid authorization credentials are required for the PPPoE connection:

PPPoE Username – username to connect to the server (must match the configured on the PPPoE server);

Password – password to connect to the server (must match the configured on the PPPoE server);

PPPoE MTU/MRU – the size (in bytes) of the Maximum Transmission Unit (MTU) and Maximum Receive Unit (MRU) used for the data encapsulation while transferring it through the PPP tunnel;

PPPoE Encryption – enables the use of MPPE encryption.

IP address of the PPP interface will be displayed in the Main page next to the PPP interface statistics if it is obtained through the established PPPoE connection, otherwise “Not Connected” message will be displayed.

PPPoE tunnel reconnection routine can be initiated using the Reconnect button which is located in the Main page next to the PPP interface statistics.

Enable DMZ: The Demilitarized zone (DMZ) can be enabled and used as a place where services can be placed such as Web Servers, Proxy Servers, and E-mail Servers such that these services can still serve the local network and are at the same time isolated from it for additional security. DMZ is commonly used with the NAT functionality as an alternative for the Port Forwarding while makes all the ports of the host network device be visible from the external network side.

DMZ configuration

DMZ Management Port: Web Management Port for the Q-Net based device (TCP/IP port 80 by default) will be used for the host device if DMZ Management Port option is enabled. In this case Q-Net device will respond to the requests from the external network as if it was the host which is specified with DMZ IP. It is recommended to leave Management Port disabled while the Q-Net based device will become inaccessible from the external network if enabled.

DMZ IP: connected to the internal network host, specified with the DMZ IP address will be accessible from the external network.

LAN IP Address assigned via DHCP with IP fallback

DHCP Fallback IP: In case the external network interface of the Router is placed in Dynamic IP Address mode (DHCP) and is unable to obtain an IP address from a valid DHCP server, it will fall back to the static IP address listed here.

In case the IP settings of the Q-Net powered device are unknown, they can be retrieved with the help of the [UBNT_Discovery_Utility Ubiquiti Discovery Utility]. Multi-platform Utility should be started on the administrator PC which resides on the same network segment as the Q-Net device.

Q-Net system will return to the default IP configuration (192.168.1.20/255.255.255.0) If the Reset to defaults routine is initiated.

Multicast Routing Settings

With a multicast design, applications can send one copy of each packet and address it to the group of computers that want to receive it. This technique addresses packets to a group of receivers rather than to a single receiver. It depends on the network to forward the packets to the hosts which need to receive them. Common Routers isolate all the broadcast (thus multicast) traffic between the internal and external networks, however Q-Net provides the multicast traffic pass-through functionality.

Multicast routing enabled

Enable Multicast Routing option enables the multicast packets pass-through between internal and external networks while device is operating in Router mode. Multicast intercommunication is based on Internet Group Management Protocol (IGMP).

Firewall Settings

Firewall functionality on any router interface can be enabled using the “Enable Firewall” option. Router Firewall rules can be configured, enabled or disabled while using Firewall configuration window which is opened with the “Configure” button.

Firewall Configuration Settings

Firewall entries can be specified by using the following criteria:

Interface the interface (WLAN, LAN or PPP) where filtering of the incoming/passing-through packets is processed;

IP Type sets which particular L3 protocol type (IP, ICMP, TCP, UDP, P2P) should be filtered;

Source IP/mask is the source IP of the packet (specified within the packet header), usually it is the IP of the host system which sends the packets;

Source Port is the source port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application which sends the packets;

Destination IP/mask is the destination IP of the packet (specified within the packet header), usually it is the IP of the system which the packet is addressed to;

Destination Port is the destination port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application which the packet is addressed to.

Comments is the informal field for the comment of the particular firewall entry. Few words about the particular firewall entry purpose are saved there usually.

On flag enables or disables the effect of the particular firewall entry. All the added firewall entries are saved in system configuration file, however only the enabled firewall entries will be active during the Q-Net system operation.

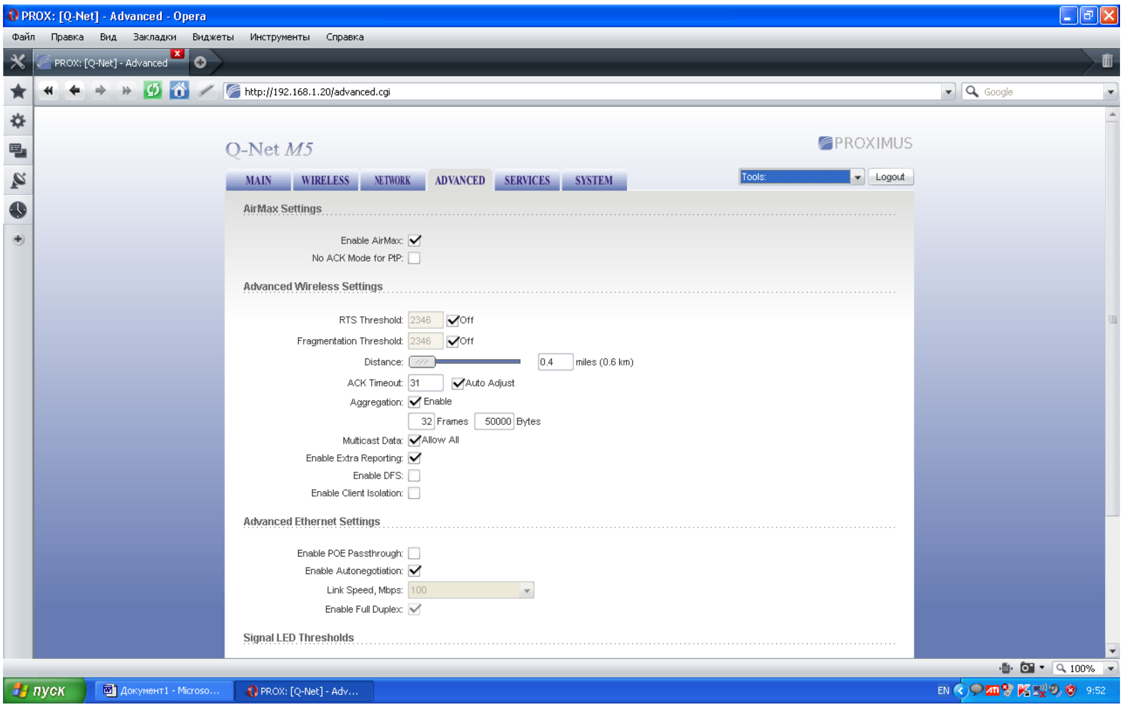
Not operators can be used for inverting the Source IP/mask, Source Port, Destination IP/mask and Destination Port filtering criteria (i.e. if not is enabled for the specified Destination Port value 443, the filtering criteria will be applied to all the packets sent to any Destination Port except the 443 which is commonly used by HTTPS).

Newly added Firewall entries can be saved by activating Save button or discarded by activating Cancel button in the Firewall configuration window.

All the active firewall entries are stored in the FIREWALL chain of the iptables filter table, while the device is operating in Router mode. Please refer to the iptables tutorial for detailed description of the firewall functionality in Router mode.

Click ***Change button*** to save the changes made in the Network page

Page “Advanced”



AirMax Settings

Enable AirMax: ☑
No ACK Mode for PtP: □

Advanced Wireless Settings

RTS Threshold: 2346 ☑Off
Fragmentation Threshold: 2346 ☑Off
Distance: 0.4 miles (0.6 km)
ACK Timeout: 31 ☑Auto Adjust
Aggregation: ☑ Enable
32 Frames 50000 Bytes
Multicast Data: ☑Allow All
Enable Extra Reporting: ☑
Enable DFS: □
Enable Client Isolation: □

Advanced Ethernet Settings

Enable POE Passthrough: □
Enable Autonegotiation: ☑
Link Speed, Mbps: 100
Enable Full Duplex: ☑

Signal LED Thresholds

Advanced

This page handles advanced routing and wireless settings. The Advanced options page allows you to manage advanced settings that influence on the device performance and behavior. The advanced wireless settings are dedicated for more technically advanced users who have a sufficient knowledge about wireless LAN technology. These settings should not be changed unless you know what effect the changes will have on your device.

AirMax: AirMax is the TDMA polling technology (Applicable only for AP or AP WDS mode). If AirMax is enabled, the device only accepts AirMax stations. AirMax also features some advanced QOS AutoDetection settings.

Advanced Wireless Setting

Rate Algorithm: defines data rate algorithm convergence:

Optimistic Algorithm is aggressive enough to move to a higher rate but yet tries to conservatively capture the fluctuations of the RSSI. It starts with the highest possible rate and then decreases till the rate can be supported while periodically transmitting packets at higher rates and computing the transmission time. The optimistic rate algorithm always looks to achieve highest throughput while sacrificing noise immunity and robustness.

Conservative Algorithm is less sensitive to individual packet failure as it is based on a function of number of successful and erroneous transmission/retransmission over a sampling period. It steps down to a lower rate after continuous packet failure and steps up after number of successful packets. The conservative rate algorithm provides the best case stability / robustness, but may compromise maximum throughput. It is recommended to select conservative rate algorithm when the signal strength is low due to noisy environment or link distance.

EWMA Algorithm is trying to move to a higher rate but is continuously monitoring the packet failure counters. The Exponential Weighted Moving Average (EWMA) Algorithm (also known as minstrel) is a hybrid of the Conservative and Optimistic Algorithm. It is the compromise for most of the wireless network use cases.

Noise Immunity option increases the robustness of the device to operate in the presence of noise disturbance which is usually generated by external traffic sources, channel hopping signals and other interferers.

RTS Threshold: determines the packet size of a transmission and, through the use of an access point, helps control traffic flow. The range is 0-2347bytes, or word "off". The default value is 2347 which means that RTS is disabled.

RTS and Fragmentation Threshold

RTS/CTS (Request to Send / Clear to Send) is the mechanism used by the 802.11 wireless networking protocol to reduce frame collisions introduced by the hidden terminal problem. RTS/CTS packet size threshold is 0-2347 bytes. If the packet size the node wants to transmit is larger than the threshold, the RTS/CTS handshake gets triggered. If the packet size is equal to or less than threshold the data frame gets sent immediately.

System uses Request to Send/Clear to Send frames for the handshake which provide collision reduction for access point with hidden stations. The stations are sending a RTS frame first while data is send only after handshake with an AP is completed. Stations respond with the CTS frame to the RTS which provides clear media for the requesting station to send the data. CTS collision control management has time interval defined during which all the other stations hold off the transmission and wait until the requesting station will finish transmission.

Fragmentation Threshold: specifies the maximum size for a packet before data is fragmented into multiple packets. The range is 256-2346 bytes, or word "off". Setting the Fragmentation Threshold too low may result in poor network performance.

The use of fragmentation can increase the reliability of frame transmissions. Because of sending smaller frames, collisions are much less likely to occur. However lower values of the Fragmentation Threshold will result lower throughput as well. Minor or no modifications of the Fragmentation Threshold value is recommended while default setting of 2346 is optimum in most of the wireless network use cases.

Q-Net has an auto-acknowledgement timeout algorithm which dynamically optimizes the frame acknowledgement timeout value without user intervention. This is a critical feature required for stabilizing long-distance outdoor links. The user also has the ability to enter the value manually.

Distance and ACK Timeout

Distance: specify the distance value in miles (or kilometers) using slider or enter the value manually. The signal strength and throughput falls off with range. Changing the distance value will change the ACK Timeout to the appropriate value of the distance.

ACK Timeout: specify the ACK Timeout. Every time the station receives the data frame it sends an ACK frame to the AP (if transmission errors are absent). If the station receives no ACK frame from the AP within set timeout it re-sends the frame. The performance drops because of the too many data frames are re-send, thus if the timeout is set too short or too long, it will result poor connection and throughput performance.

Changing the ACK Timeout"== value will change the Distance to the appropriate distance value for the ACK Timeout.

Auto Adjust control will enable the ACK Timeout Self-Configuration feature. If enabled, ACK Timeout value will be derived dynamically using an algorithm similar to the Conservative Rate

Algorithm described above. It is not recommended to use Auto Adjust option for long range links if the signal level is low or the high level of interference is present.

If two or more stations are located at the considerably different distance from the Access Point the are associated to, the highest ACK Timeout for the farthest station should be set at the AP side. It is not recommended to use Auto Adjust option for Point-to-Multipoint connections as it will not warrant highest network performance in all the use cases.

SuperG Features: select the options to enable the chosen SuperG features which increase the network performance:

Fast Frame – frame aggregation and timing modifications which increases the data throughput.

Bursting – more data frames per given time period are transmitted thus the data throughput is increased.

Compression – real-time hardware data compression is enabled which allows more data sent per frame.

Multicast Data and Rate

Multicast Data: This option allows the Multicast packet pass-through functionality. By default this option is disabled.

Multicast Rate: This option allows Multicast packets to be sent in higher rates (up to the 54 Mbps) than commonly used (up to 6 Mbps). Both Q-Net based devices the sender (Station) and the receiver (Access Point) must have the same Multicast Rate configured in order to achieve better multicast packet throughput performance.

Enable Extra Reporting

Enable Extra Reporting: feature will report additional information (i.e. Host Name) in management frames. This information is commonly used for system identification and status reporting in discovery utilities and Router operating systems.

Enable Client Isolation: This option allows packets only to be sent from the external network to the CPE and vice verse (applicable for AP/AP WDS mode only). If the Client Isolation is enabled wireless stations connected to the same AP will not be able to interconnect on both layer 2 (MAC) and layer 3 (IP) level. This is effective for the associated stations and WDS peers also.

LED Thresholds

LED Thresholds Configuration

The LED's on the back of the Q-Net Device can be made to light on when received signal levels reach the values defined in the following fields. This allows a technician to easily deploy an Q-Net CPE without logging into the unit (i.e. for antenna alignment operation).

Signal LED Thresholds specify the marginal value of Signal Strength (dBm) which will switch on LEDs indicating signal strength:

LED 1 (Red) will switch on if the Signal Strength reaches the value set in an entry field next to it.

LED 2 (Yellow) will switch on if the Signal Strength reaches the value set in an entry field next to it.

LED 3 (Green) will switch on if the Signal Strength reaches the value set in an entry field next to it.

LED 4 (Green) will switch on if the Signal Strength reaches the value set in an entry field next to it.

Configuration example: if the Signal Strength (displayed in the Main page) fluctuates around -63 dBm, the LED Thresholds can be set to the values -70, -65, -62, -60. Note: sign "-" character should not be used for the Signal Strength value specification.

Wireless Traffic Shaping

Wireless Traffic shaping feature is dedicated for upstream and downstream bandwidth control while looking from the client (connected on Ethernet interface) perspective.

The traffic can be limited at the Q-Net based device in the upload and download direction based on a user defined rate limit. This is layer 3 QoS.

Enable Traffic Shaping: control will enable bandwidth control on the device.

Incoming Traffic Limit: specify the maximum bandwidth value (in kilobits per second, Kbps) for traffic passing from wireless interface to Ethernet interface.

Incoming Traffic Burst: specify the data volume (in kilobytes) to which Incoming Traffic Limit will not be effective afterwards data connection is initiated.

Outgoing Traffic Limit: specify the maximum bandwidth value (in kilobits per second, Kbps) for traffic passing from Ethernet interface to wireless interface.

Outgoing Traffic Burst: specify the data volume (in kilobytes) to which Outgoing Traffic Limit will not be effective afterwards data connection is initiated.

QoS

Quality of Service is a component of the wireless LAN standard for quality of service (QoS). The QoS assigns priority to the selected network traffic, prevents packet collisions and delays thus improving VoIP calls and watching video over WLANs.

QoS Level: choose the type of the network traffic to which the priority will be set or disable the QoS feature.

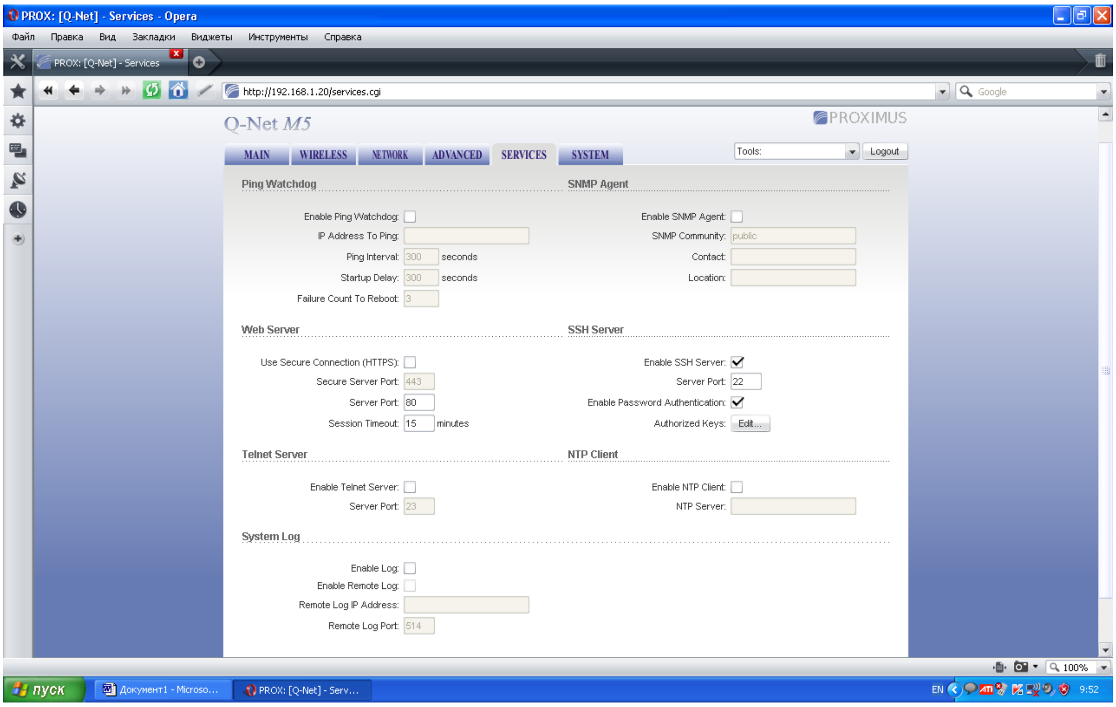
No QoS – disable QoS.

Auto Priority – priority of traffic is assigned automatically according to the type of the passing through data.

Voice Priority – enable priority of the voice traffic for all the passing through data.

Video Priority – enable priority of the video traffic for all the passing through data.

Page "Services"


PROX: [Q-Net] - Services - Opera
Файл Правка Вид Закладки Виджеты Инструменты Справка
PROX: [Q-Net] - Services
http://192.168.1.20/services.cgi
Google
Q-Net M5
PROXIMUS
MAIN WIRELESS NETWORK ADVANCED SERVICES SYSTEM
Tools:
Logout
100%
пуск
Документ1 - Microso...
PROX: [Q-Net] - Serv...
EN
9:52

Ping Watchdog

Enable Ping Watchdog: □
IP Address To Ping:
Ping Interval: 300 seconds
Startup Delay: 300 seconds
Failure Count To Reboot: 3

SNMP Agent

Enable SNMP Agent: □
SNMP Community: public
Contact:
Location:

Web Server

Use Secure Connection (HTTPS): □
Secure Server Port: 443
Server Port: 80
Session Timeout: 15 minutes

SSH Server

Enable SSH Server: ☑
Server Port: 22
Enable Password Authentication: ☑
Authorized Keys: Edit...

Telnet Server

Enable Telnet Server: □
Server Port: 23

NTP Client

Enable NTP Client: □
NTP Server:

System Log

Enable Log: □
Enable Remote Log: □
Remote Log IP Address:
Remote Log Port: 514

Services Page

Ping WatchDog

The ping watchdog sets the Q-Net Device to continuously ping a user defined IP address (it can be the internet gateway for example). If it is unable to ping under the user defined constraints, the Q-Net device will automatically reboot. This option creates a kind of “fail-proof” mechanism.

Ping Watchdog is dedicated for continuous monitoring of the particular connection to remote host using the Ping tool. The Ping works by sending ICMP “echo request” packets to the target host and listening for ICMP “echo response” replies. If the defined number of replies is not received, the tool reboots the device.

Enable Ping Watchdog: control will enable Ping Watchdog Tool.

IP Address to Ping: specify an IP address of the target host which will be monitored by Ping Watchdog Tool.

Ping Interval: specify time interval (in seconds) between the ICMP “echo requests” are sent by the Ping Watchdog Tool.

Startup Delay: specify initial time delay (in seconds) until first ICMP “echo requests” are sent by the Ping Watchdog Tool.

The value of Startup Delay should be at least 60 seconds as the network interface and wireless connection initialization takes considerable amount of time if the device is rebooted.

Failure Count to Reboot: specify the number of ICMP “echo response” replies. If the specified number of ICMP “echo response” packets is not received continuously, the Ping Watchdog Tool will reboot the device.

SNMP Agent

Simple Network Monitor Protocol (SNMP) is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. Q-Net contains an SNMP agent which allows it to communicate to SNMP manage applications for network provisioning.

SNMP Agent provides an interface for device monitoring using the Simple Network Management Protocol (an application layer protocol that facilitates the exchange of management information between network devices). SNMP Agent allows network administrators to monitor network performance, find and solve network problems. For the purpose of equipment identification, it is always a good idea to configure SNMP agents with contact and location information:

Enable SNMP Agent: control will enable SNMP Agent.

SNMP Community: specify SNMP community string. It is required to authenticate access to MIB objects and functions as embedded password. The device supports a Read-only community string that gives read access to authorized management stations to all the objects in the MIB except the community strings, but does not allow write access. Q-Net supports SNMP v1.

Contact: specify the identity or the contact who should be contacted in case a emergency situation arise.

Location: specify the physical location of the device.

NTP Client

NTP Client: The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. It can be used to set the Q-Net system time. System Time is reported next to the every System Log entry while registering system events if Log option is enabled.

Enable NTP Client: control will enable NTP client.

***NTP Server:* specify** the IP address or domain name of the NTP Server.

Web Server

***Web Server:* the** following Q-Net Device Web Server parameters can be set there:

Use Secure Connection (HTTPS): If checked Web server will use secure HTTPS mode. HTTPS mode is unchecked by default.

Secure Server Port: Web Server TCP/IP port setting while using HTTPS mode.

Server Port: Web Server TCP/IP port setting while using HTTP mode.

Telnet Server

Telnet Server: the following Q-Net Device Telnet Server parameters can be set there:

Enable Telnet Server: This option activates the Telnet access to the Q-Net Device.

Server Port: Telnet service TCP/IP port setting.

SSH Server

SSH Server: the following Q-Net Device SSH Server parameters can be set there:

Enable SSH Server: This option enables SSH access to the Q-Net Device.

Server Port: SSH service TCP/IP port setting.

System Log

Enable Log **:** This option enables the registration routine of the system log messages.

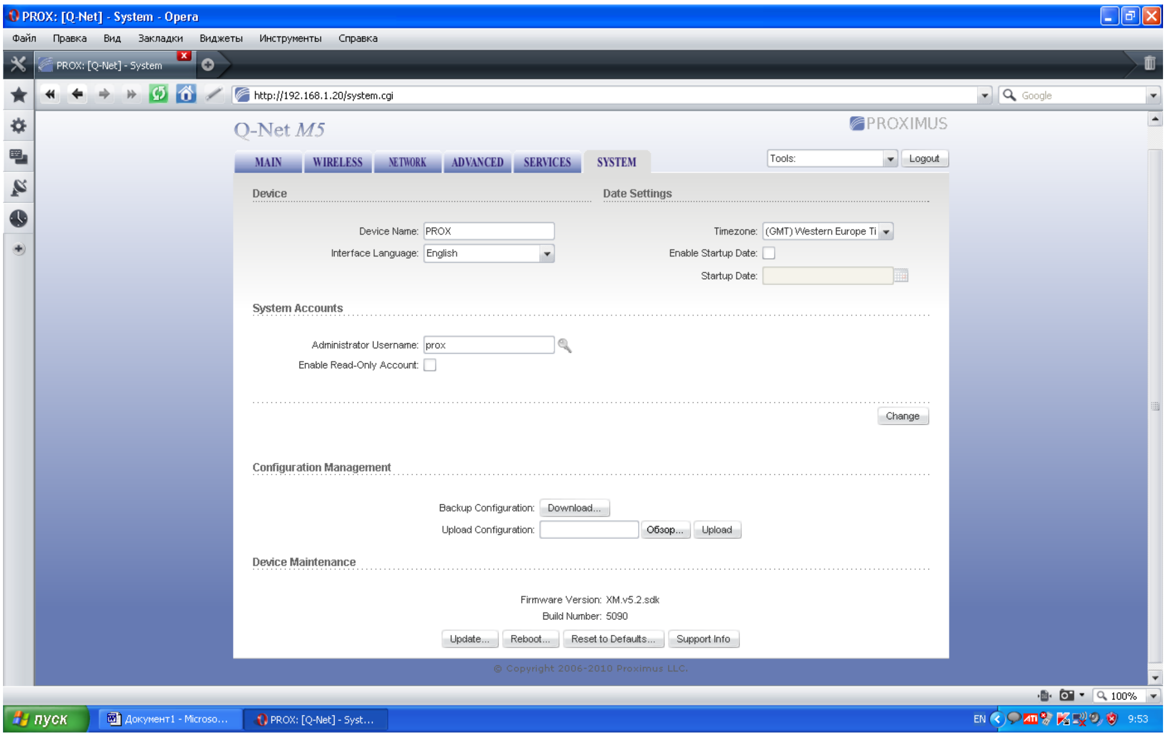
Enable Remote Log: enables the syslog remote sending function while System log messages are sent to a remote server specified by the Remote Log IP Address and Remote Log Port.

***Remote Log IP Address* is** the host IP address where syslog messages should be sent. Remote host should be configured properly to receive syslog protocol messages.

Remote Log Port: is the TCP/IP port of the host syslog messages should be sent. “514” is the default port for the commonly used system message logging utilities.

Every logged message contains at least a System Time and a Host Name. Usually a particular service name which generates the system event is specifies also within the message. Messages from different services have different context and different level of the details. Usually error, warning or informational system services messages are reported, however more detailed Debug level messages can be reported also. The more detailed system messages are reported, the greater volume of log messages will be generated.

Page “System”



Device

Device Name: PROX

Interface Language: English

Date Settings

Timezone: (GMT) Western Europe Ti

Enable Startup Date: □

Startup Date:

System Accounts

Administrator Username: prox

Enable Read-Only Account: □

Configuration Management

Backup Configuration: Download...

Upload Configuration:

Device Maintenance

Firmware Version: XM.v5.2.sdk

Build Number: 5090

The System Page contains Administrative options. This page enables administrator to customize, reboot the device, set it to factory defaults, upload a new firmware, backup or update the configuration and configure administrator’s credentials.

Firmware

Use this section to find out current software version and update the device with the new firmware. The device firmware update is compatible with all configuration settings. System configurations are preserved while the device is updated with a new firmware version.

Firmware version: displays the version of the current firmware of the Q-Net system.

Upgrade: button opens the Firmware Upload window if activated.

Firmware Upgrade

Current Firmware: displays the version of the Q-Net firmware which is currently operating.

Firmware File: activate Browse button to navigate to and select the new firmware file. The full path to the new firmware file location can be specified there. New firmware file is transferred to the system after Upload button is activated.

Close this window **–** button cancels the new firmware upload process if activated.

Upgrade button should be activated in order to proceed with firmware upgrade routine (new firmware image should be uploaded into the system first). Please be patient, as the firmware upgrade routine can take 3-7 minutes. Q-Net based device will be inaccessible until the firmware upgrade routine is completed.

Do not switch off, do not reboot and do not disconnect the device from the power supply during the firmware upgrade process as these actions will damage the device!

Close this window **–** button closes the firmware upgrade window if activated. This action will not cancel the firmware upgrade process.

Host Name

Host Name is the system wide device identifier. It is reported by SNMP Agent to authorized management stations. Host Name will be represented in popular Router Operating Systems registration screens and discovery tools.

Host Name: specifies the system identity.

Change button saves the ***Host Name*** if activated.

Administrative Account

In this section you can modify the administrator password to protect your device from unauthorized configuration. The default administrator's password should be changed on the very first system setup:

Administrator Username: specifies the name of the system user.

Current Password: administrator is required to enter a current password. It is required for *Password* or *Administrator Username* change routine.

Default administrator login credentials**:**

- User Name: prox
- Password: prox

New Password: new password used for administrator authentication should be specified.

Verify Password: new password should be re-entered to verify its accuracy.

Click ***Change*** button to save the changes.

Read-only Account

In this section you can enable the read-only account, and configure the username and password to protect your device from unauthorized access. The default option is disabled.

Enable Read-Only Account: This option activates the read-only account.

Read-Only Username: specifies the name of the system user.

Password: new password used for read-only administrator authentication should be specified.

Interface Language

Interface Language, by default: English

Q-Net supports multiple languages in the Web Management Interface.

Language options change the look and feel of the Web Management Interface while renaming the labels of all the configuration settings and controls according to the translation in particular language. The default language is English. The colors and the layout of all the web elements are not changed after the change of the language.

Language selection is saved by activating the ***Set as default*** button.

Logo Customization

Use the controls in this section to configure custom logo on the device web management interface. The logo must conform to these limitations:

- The volume size of the logo is 50 Kilobytes or less;
- The maximum height of logo should be 70 pixels;
- Only .gif format images are accepted.

To upload new logo, enable logo customization and specify the location of logo file:

Enable Custom Logo: control will enable logo customization. If the *Enable Custom Logo* option is not selected the default Ubiquiti logo will be set/restored and the custom logo will be removed.

Logo Target URL: the target URL of custom logo can be specified in this field. Target URL is opened when clicking on custom logo.

Logo File: *activate* ***Browse*** button to navigate to and select the logo file. The full path to the logo file stored locally can be specified there. Logo file is transferred to the system after ***Upload*** button is activated.

Default Logo

If the logo file maximum volume size (50 kilobytes) is exceeded the system performance issues may occur. Default logo dimension (in pixels) is 114 (width) X 53(height).

Configuration Management

Q-Net configuration is stored in plain text file. Use the *Configuration Management* section controls to backup, restore or update the system configuration file:

Backup Configuration: click ***Download*** button to download the current system configuration file.

Upload Configuration: click ***Browse*** button to navigate to and select the new configuration file or specify the full path to the configuration file location.

Activating the ***Upload*** button will transfer new configuration file to the system. The settings of the new configuration will be visible in the *Link Setup*, *Network*, *Advanced*, *Services* and *System* pages of the Web Management Interface.

New configuration will be effective after the ***Apply*** button is activated and system reboot cycle is completed. Previous system configuration is deleted after ***Apply*** button is activated. It is highly recommended to backup the system configuration before uploading the new configuration.

Device Maintenance

The controls in this section are dedicated for the device maintenance routines: rebooting, resetting, generating of the support information report.

Reboot: activate ***Reboot*** control in order to initiate full reboot cycle of the device. Reboot effect is the same as the hardware reboot which is similar to the power off - power on cycle. The system configuration is not modified after the reboot cycle completes. Any non-applied changes will be lost.

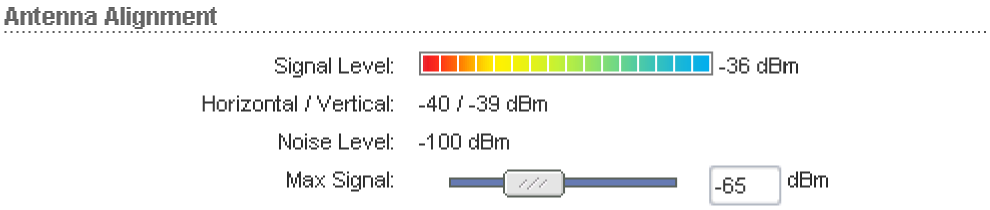
Reset to Defaults: activate ***Reset to Defaults*** control in order to initiate reset the device to factory defaults routine. Reset routine initiates system ***Reboot*** process (similar to the power off - power on cycle). The running system configuration will be deleted and the default system configuration (all the system settings with no exception) will be set.

After the ***Reset to Defaults*** routine is completed, Q-Net system will return to the default IP configuration **(192.168.1.20/255.255.255.0)** and will start operating in ***Station-Bridge*** mode. It is highly recommended to backup the system configuration before the ***Reset to Defaults*** is initiated.

Support Info: *activate Support Info button in order to get system information file. This file should be provided to Ubiquiti support engineers (upon the request) while investigating all the technical support or configuration issues if any.*

Tools

Align Antenna utility allows the installer to point and optimize the antenna in the direction of maximum link signal.



Antenna Alignment

Signal Level: -36 dBm

Horizontal / Vertical: -40 / -39 dBm

Noise Level: -100 dBm

Max Signal: -65 dBm

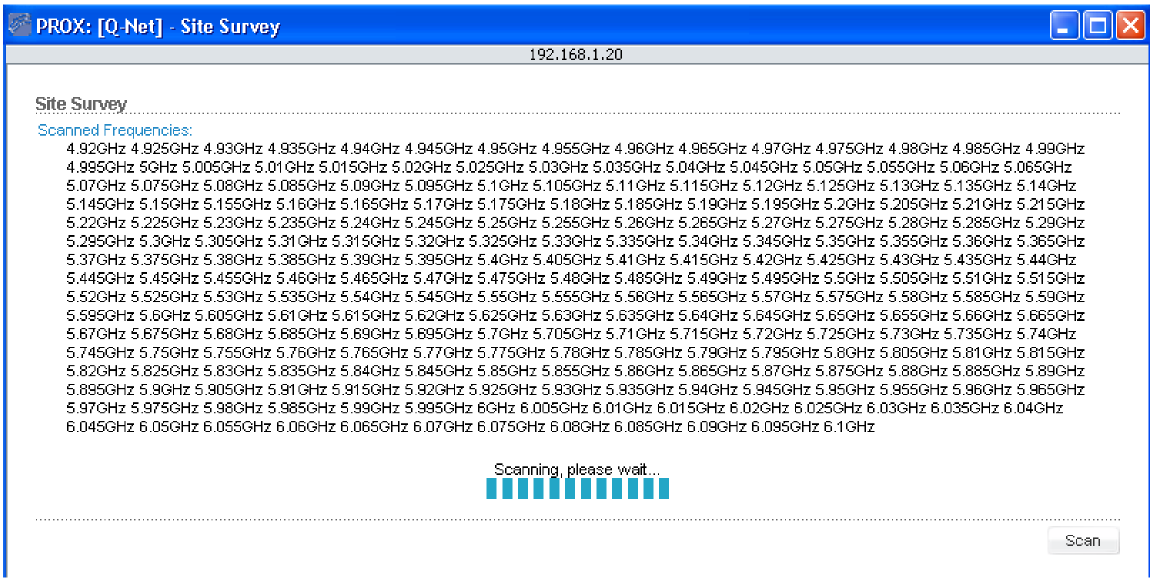
Selection of the Align Antenna tool will open new window with signal strength indicator. Window reloads every second displaying the signal strength of the last received packet.

The “RSSI Range” slider bar allows the range of the meter to be either increased or reduced. If the range is reduced, the color change will be more sensitive to signal fluctuations as RSSI Range slider actually changes an offset of the maximum indicator value thus the scale itself.

“Noise Level”: value displays the value of the noise level wireless signal was received.

***Align Antenna* window can be closed with the Close this window button.**

Site Survey: utility will search for wireless networks in range on all the supported channels while device is operating in Access Point or Station mode. In Station mode channel list can be modified. Refer to the section Link Setup for the details on channel list customization.



PROX: [Q-Net] - Site Survey

192.168.1.20

Site Survey

Scanned Frequencies:

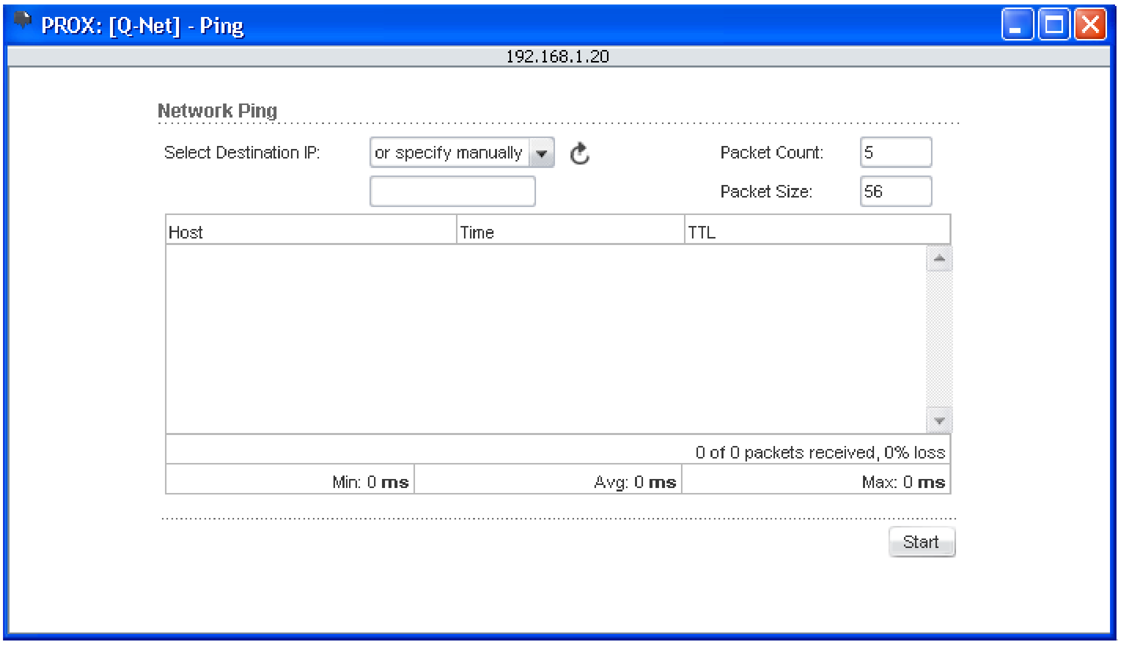
```
4.92GHz 4.925GHz 4.93GHz 4.935GHz 4.94GHz 4.945GHz 4.95GHz 4.955GHz 4.96GHz 4.965GHz 4.97GHz 4.975GHz 4.98GHz 4.985GHz 4.99GHz
4.995GHz 5GHz 5.005GHz 5.01GHz 5.015GHz 5.02GHz 5.025GHz 5.03GHz 5.035GHz 5.04GHz 5.045GHz 5.05GHz 5.055GHz 5.06GHz 5.065GHz
5.07GHz 5.075GHz 5.08GHz 5.085GHz 5.09GHz 5.095GHz 5.1GHz 5.105GHz 5.11GHz 5.115GHz 5.12GHz 5.125GHz 5.13GHz 5.135GHz 5.14GHz
5.145GHz 5.15GHz 5.155GHz 5.16GHz 5.165GHz 5.17GHz 5.175GHz 5.18GHz 5.185GHz 5.19GHz 5.195GHz 5.2GHz 5.205GHz 5.21GHz 5.215GHz
5.22GHz 5.225GHz 5.23GHz 5.235GHz 5.24GHz 5.245GHz 5.25GHz 5.255GHz 5.26GHz 5.265GHz 5.27GHz 5.275GHz 5.28GHz 5.285GHz 5.29GHz
5.295GHz 5.3GHz 5.305GHz 5.31GHz 5.315GHz 5.32GHz 5.325GHz 5.33GHz 5.335GHz 5.34GHz 5.345GHz 5.35GHz 5.355GHz 5.36GHz 5.365GHz
5.37GHz 5.375GHz 5.38GHz 5.385GHz 5.39GHz 5.395GHz 5.4GHz 5.405GHz 5.41GHz 5.415GHz 5.42GHz 5.425GHz 5.43GHz 5.435GHz 5.44GHz
5.445GHz 5.45GHz 5.455GHz 5.46GHz 5.465GHz 5.47GHz 5.475GHz 5.48GHz 5.485GHz 5.49GHz 5.495GHz 5.5GHz 5.505GHz 5.51GHz 5.515GHz
5.52GHz 5.525GHz 5.53GHz 5.535GHz 5.54GHz 5.545GHz 5.55GHz 5.555GHz 5.56GHz 5.565GHz 5.57GHz 5.575GHz 5.58GHz 5.585GHz 5.59GHz
5.595GHz 5.6GHz 5.605GHz 5.61GHz 5.615GHz 5.62GHz 5.625GHz 5.63GHz 5.635GHz 5.64GHz 5.645GHz 5.65GHz 5.655GHz 5.66GHz 5.665GHz
5.67GHz 5.675GHz 5.68GHz 5.685GHz 5.69GHz 5.695GHz 5.7GHz 5.705GHz 5.71GHz 5.715GHz 5.72GHz 5.725GHz 5.73GHz 5.735GHz 5.74GHz
5.745GHz 5.75GHz 5.755GHz 5.76GHz 5.765GHz 5.77GHz 5.775GHz 5.78GHz 5.785GHz 5.79GHz 5.795GHz 5.8GHz 5.805GHz 5.81GHz 5.815GHz
5.82GHz 5.825GHz 5.83GHz 5.835GHz 5.84GHz 5.845GHz 5.85GHz 5.855GHz 5.86GHz 5.865GHz 5.87GHz 5.875GHz 5.88GHz 5.885GHz 5.89GHz
5.895GHz 5.9GHz 5.905GHz 5.91GHz 5.915GHz 5.92GHz 5.925GHz 5.93GHz 5.935GHz 5.94GHz 5.945GHz 5.95GHz 5.955GHz 5.96GHz 5.965GHz
5.97GHz 5.975GHz 5.98GHz 5.985GHz 5.99GHz 5.995GHz 6GHz 6.005GHz 6.01GHz 6.015GHz 6.02GHz 6.025GHz 6.03GHz 6.035GHz 6.04GHz
6.045GHz 6.05GHz 6.055GHz 6.06GHz 6.065GHz 6.07GHz 6.075GHz 6.08GHz 6.085GHz 6.09GHz 6.095GHz 6.1GHz
```

Scanning, please wait...

Site Survey reports MAC Address, ‘’ESSID’’, Encryption type (if any), Signal Strength (dBm), Frequency (GHz) and wireless channel of all the surrounding Access Points which can be found by the Q-Net M5 based device.

The Site Survey can be updated using the Scan button. Site Survey window can be closed with the Close this window button.

Ping: This utility will ping other devices on the network directly from the Q-Net M5 device.



PROX: [Q-Net] - Ping

192.168.1.20

Network Ping

Select Destination IP: or specify manually

Packet Count: 5

Packet Size: 56

Host	Time	TTL

0 of 0 packets received, 0% loss

Min: 0 ms Avg: 0 ms Max: 0 ms

Ping utility should be used for the preliminary link quality and packet latency estimation between two network devices using the ICMP packets.

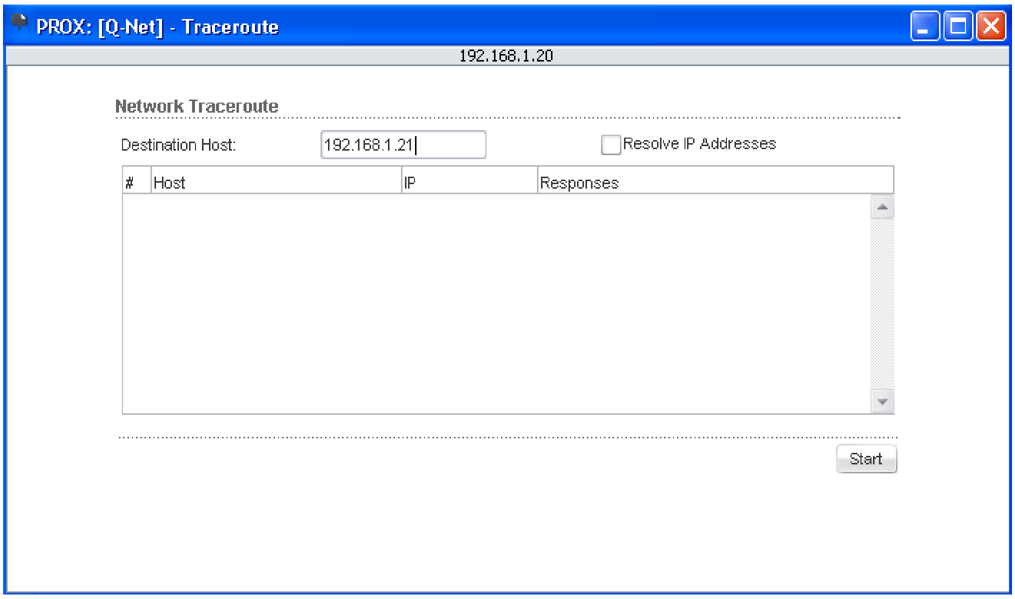
Remote system IP can be selected from the list which is generated automatically (Select destination IP) or can be specified manually.

The size of the ICMP packets can be specified in the Packet size field. Estimation is done after the number of ICMP packets (specified in Packet count field) is transmitted/received.

Packet loss statistics and latency time evaluation is provided after the test is completed.

The test is started using the Start button.

TraceRoute: Allows tracing the hops from the Q-Net M5 device to a selected outgoing IP address. It should be used for the finding the route taken by ICMP packets across the network to the Destination host.



PROX: [Q-Net] - Traceroute

192.168.1.20

Network Traceroute

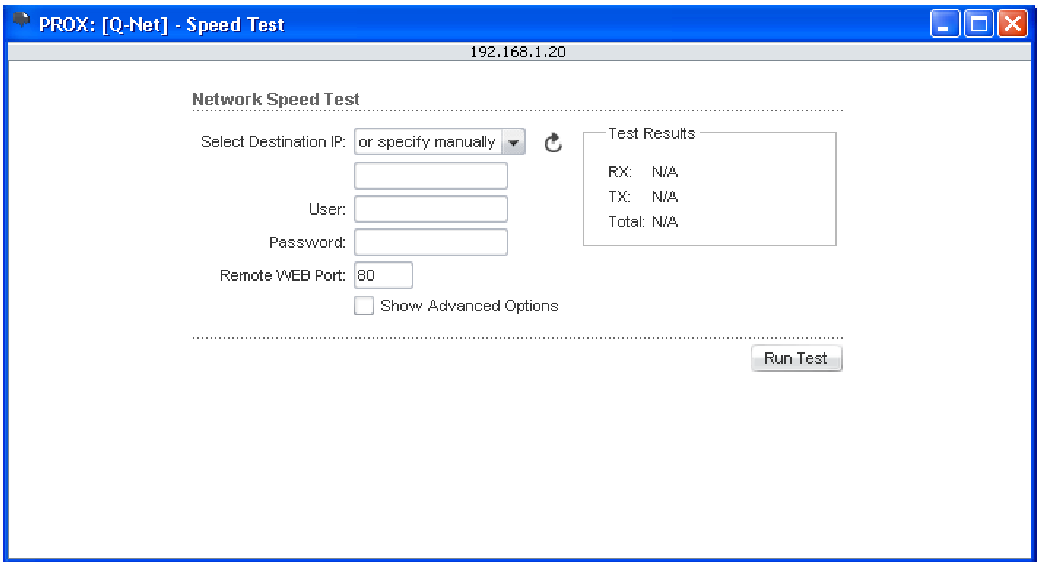
Destination Host: 192.168.1.21

☐ Resolve IP Addresses

#	Host	IP	Responses

Resolution of the IP addresses (symbolically rather than numerically) can be enabled by selecting the Resolve IP address option. The test is started using the Start button.

Speed Test. This utility allows for testing the connection speed to and from any reachable IP address on the Q-Net M5 device network. It should be used for the preliminary throughput estimation between two network devices. If both devices are powered by Q-Net M5, the estimation is more precise, otherwise only rough estimation is provided while using ICMP packet exchange routines.



PROX: [Q-Net] - Speed Test

192.168.1.20

Network Speed Test

Select Destination IP: or specify manually

User:

Password:

Remote WEB Port: 80

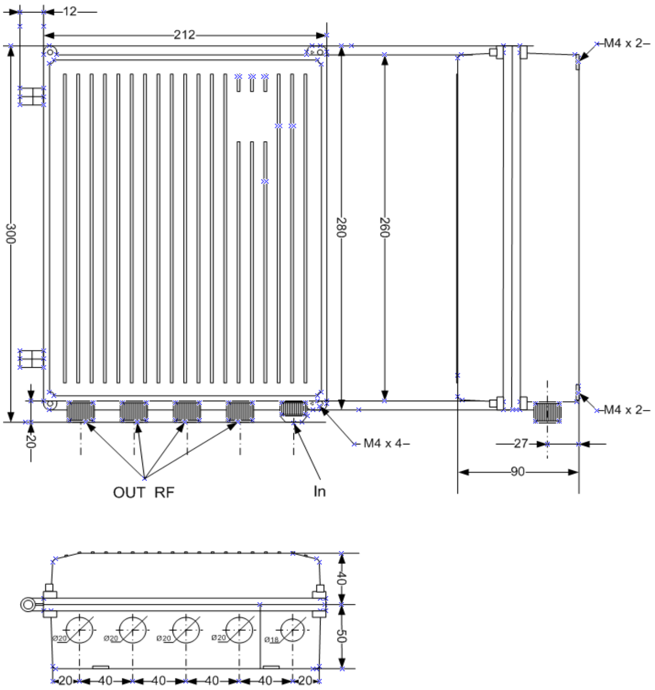
□ Show Advanced Options

Test Results

RX: N/A
TX: N/A
Total: N/A

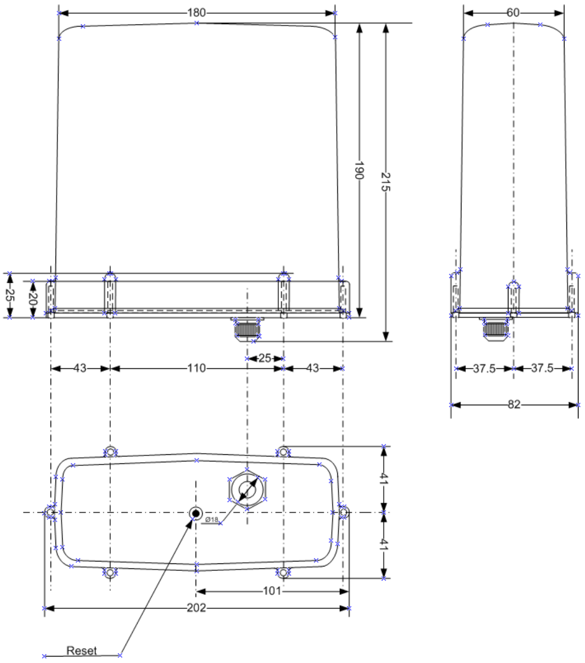
Q-Net Access Point Specifications

Frequency Band, MHz	1300-1700 MHz, 2300-2400 MHz and 2500-2700 MHz
Frequency step, MHz	5
Duplex	TDD
Channel Width, MHz	5,10,20,40
Radio Technology	Orthogonal Frequency Division Multiplexing (OFDM)
Modulation Type	64QAM, 16QAM, QPSK, BPSK
Frequency selection	software
Max.Transmit Output Power,dBm	27
Receiver Sensitivity, dBm	-96
Dynamic Range,dB	74
Wireless Security	WEP, WPA, WPA 2
Wireless Mode	Access Point, Access Point WDS
Effective range ,km	Up to 10 (direct LOS, antenna gain>23 dBi)
Antenna	16 dbi (internal)
Polarization	Dual Linear
Cross-pol Isolation	22 dB min
VSWR	1,6:1
H-pol Beamwidth, deg	43
V-pol Beamwidth, deg	41
Networking Interface (LAN)	Ethernet, 10/100 Base-T
Network Mode	Bridge,Router
Device Management	HTTP,HTTPS,Telnet,SSH,SNMP
Size, mm(L/H/W)	300/90/224
Weight, kg	1,8
Max. Power Consumption, W	12
Power Supply	24V, 0.5A surge portection integrated POE adapter
Power Method	Passive Power over Ethernet (pairs 4,5+; 7,8 return)
Operating Temperature, oC	-30 to 80
Operating Humidity,%	5 to 95
Frequency step, MHz	5
Duplex	TDD
Channel Width, MHz	5,10,20
Radio Technology	Orthogonal Frequency Division Multiplexing (OFDM)
Modulation Type	64QAM, 16QAM, QPSK, BPSK
Frequency selection	software
Max.Transmit Output Power,dBm	29
Receiver Sensitivity, dBm	-92
Dynamic Range,dB	70
Wireless Security	WEP, WPA, WPA 2
Wireless Mode	Access Point, Access Point WDS
Effective range ,km	Up to 30 (direct LOS, antenna gain>20 dBi)
Antenna	14 dbi (external)
RF Connector	N-type Male
Networking Interface (LAN)	Ethernet, 10/100 Base-T
Network Mode	Bridge,Router
Device Management	HTTP,HTTPS,Telnet,SSH,SNMP
Size, mm(L/H/W)	300/90/224
Weight, kg	1,8
Max. Power Consumption, W	32
Power	AC~100-240V
Operating Temperature, oC	-20 to 65
Operating Humidity,%	5 to 95


12
212
M4 x 2
300
280
260
20
M4 x 4
M4 x 2
27
90
OUT RF
In
40
50
Ø20
Ø20
Ø20
Ø20
Ø18
20
40
40
40
40
40
20

Q-Net Subscriber Unit Specification

Frequency Band, MHz	1300-1700 MHz, 2300-2400 MHz and 2500-2700 MHz
Frequency step, MHz	5
Duplex	TDD
Channel Width, MHz	5,10,20,40
Radio Technology	Orthogonal Frequency Division Multiplexing (OFDM)
Modulation Type	64QAM, 16QAM, QPSK, BPSK
Frequency selection	software
Max.Transmit Output Power,dBm	23
Receiver Sensitivity, dBm	-96
Dynamic Range,dB	74
Wireless Security	WEP, WPA, WPA 2
Wireless Mode	Access Point, Access Point WDS
Effective range ,km	Up to 10 (direct LOS, antenna gain>24 dBi)
Antenna	13 dbi (internal)
Polarization	Dual Linear
Cross-pol Isolation	20 dB min
VSWR	1,4:1
H-pol Beamwidth, deg	45
V-pol Beamwidth, deg	45
Networking Interface (LAN)	Ethernet, 10/100 Base-T
Network Mode	Bridge,Router
Device Management	HTTP,HTTPS,Telnet,SSH,SNMP
Size, mm(L/H/W)	200/40/140
Weight, kg	1,2
Max. Power Consumption, W	10
Power Supply	15V, 0.8A surge portection integrated POE adapter
Power Method	Passive Power over Ethernet (pairs 4,5+; 7,8 return)
Operating Temperature, oC	-30 to 80
Operating Humidity,%	5 to 95
Frequency step, MHz	5
Duplex	TDD
Channel Width, MHz	5,10,20
Radio Technology	Orthogonal Frequency Division Multiplexing (OFDM)
Modulation Type	64QAM, 16QAM, QPSK, BPSK
Frequency selection	software
Max.Transmit Output Power,dBm	29
Receiver Sensitivity, dBm	-92
Dynamic Range,dB	70
Wireless Security	WEP, WPA, WPA 2
Wireless Mode	Station, Station WDS
Effective range ,km	Up to 30 (direct LOS, antenna gain>20 dBi)
Antenna	13,5 dbi (internal)
Networking Interface (LAN)	Ethernet, 10/100 Base-T
Network Mode	Bridge,Router
Device Management	HTTP,HTTPS,Telnet,SSH,SNMP
Size, mm(L/H/W)	215/82/202
Weight, kg	1,2
Max. Power Consumption, W	8
Power Supply	PoE (Power ower Ethernet), 18VDC
Operating Temperature, oC	-20 to 65
Operating Humidity,%	5 to 95

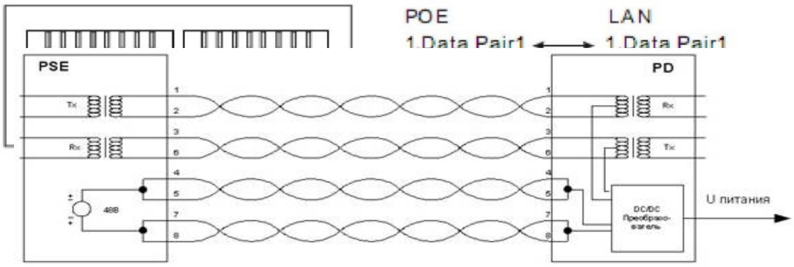

180
60
190
215
25
20
43
110
25
43
37.5
37.5
82
41
41
Ø18
101
202
Reset

Power Injector (POE Adapter)

Technical Specifications:

- Input: 100-240V AC
- line frequency: 50/60Hz
- Input current: 100VAC 0.5A maximum
- Protection: internal primary current fuse, inrush limiting
- Output voltage: 18V DC
- Load regulation: +-2%
- Maximum power: 72W
- Ripple and noise: 1% max (peak to peak)
- Transistant response: 0.5ms for 50% load change, typical
- Topology: switching-fixed frequency Flyback
- Efficiency: 70% min (meets EUP, CEC)
- Di-electrical: 3,000V AC
- Case material: PC 94V0 (Polycarbonate) RoHs compliant

- Cord and connector: Dual RJ45 Jacks(LAN +POE)


POE
LAN
1.Data Pair1
1.Data Pair1
PSE
PD
Tx
Rx
Rx
Tx
1
2
3
6
4
5
7
8
48B
DC/DC
Преобразо-
ватель
U питания